PSI Handbook of Business Security, Volumes 1 & 2

Edited by
W. Timothy Coombs

PRAEGER SECURITY INTERNATIONAL

PSI Handbook of Business Security

PSI Handbook of Business Security

VOLUME ONE

SECURING THE ENTERPRISE

EDITED BY W. TIMOTHY COOMBS

Praeger Security International
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

PSI handbook of business security / edited by W. Timothy Coombs.
2 v. ; cm.
Includes bibliographical references and index.
Contents: v. 1. Securing the enterprise—v. 2. Securing people and processes.
ISBN 978-0-275-99394-8 (set : alk. paper) — ISBN 978-0-275-99395-5 (vol. 1 : alk. paper) — ISBN 978-0-275-99396-2 (vol. 2 : alk. paper)
1. Industries—Security measures. I. Coombs, W. Timothy. II. Title: Handbook of business security.
HV8290.P77 2008
658.4'7—dc22 2007040469

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2007040469

ISBN-13: 978-0-275-99394-8 (set)
978-0-275-99395-5 (vol. 1)
978-0-275-99396-2 (vol. 2)

First published in 2008

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the United States of America

The paper used in this book complies with the
Permanent Paper Standard issued by the National
Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

CONTENTS

VOLUME 1: SECURING THE ENTERPRISE

INFORMATION (CYBER) PROTECTION

TERRORISM AS A BUSINESS SECURITY AND SAFETY CONCERN

GENERAL SAFETY CONCERNS

UNCOMMON BUSINESS SECURITY CONCERNS

VOLUME 2: SECURING PEOPLE AND PROCESSES

PHYSICAL PROTECTION

SECURITY ON A GLOBAL SCALE

ENHANCING THE HUMAN SIDE OF SECURITY AND SAFETY

PREFACE

In general, security means freedom from risk, fear, doubt, or anxiety. For organizations, business security comprises the measures taken to protect people, data, physical assets, and financial and other assets. These measures help to create a safe workplace and to reduce risks. Business security further seeks to combat the various security risks faced by organizations. When these risks become a reality, people and organizations suffer. Examples include workplace violence, terror attacks, computer hacking/data loss, disruption of the supply chain, and top management engaged in illegal acts. Moreover, these “problems” draw intense coverage from the news media, which are drawn to singular, negative events. Negative publicity resulting from incidences that might have been avoided further harms an organization by damaging its reputation, which is a valuable, if intangible, resource. Business security clearly involves high stakes.

When most people think about business security, a security guard at a front desk or gate comes to mind. Others may think of the password they have to enter when they use their computers at work. Business security is much more extensive and involved than these two common reference points. The diversity of business security is a reflection of the multitude of risks that organizations face. The security guard and the computer password represent two broad areas of business security—physical security and information security—but many more areas of concern exist. There is obviously a concern for people at a location (employees, vendors, and visitors), the grounds, the building itself, and the materials in the building. Yet business security extends outside of the facility to people and businesses located near the facility, cyberspace, vendors and others in the supply chain, and so forth. These two volumes try to capture the range and complexity of business security.

The objectives of the *PSI Handbook of Business Security* are twofold. The primary objective is to create a reference tool for people involved in business security. The entries and resources identify key security concerns and provide guidance on how to handle them. This work thus serves as a resource for anyone looking to improve security in an organization.

The secondary objective is to raise people’s awareness of their role in security. If employees fail to commit to business security, the organization is at risk. What are the odds that new hires, such as fresh college graduates, know much about security or appreciate its value? Does your orientation program properly educate them on physical and information security? Do these new people read and commit themselves to abiding by the security policies in the employee handbook? Do your long-time employees understand and appreciate their role in business security? Anyone who reads the *PSI Handbook of Business Security* should realize that every employee plays an active role in keeping an organization secure.

Business security is complex and multifaceted. This set is comprised of two volumes that explore this diverse area. Volume 1 focuses on information security, terrorism, and topics related to business security that often are not included in discussions of business security. Volume 2 focuses on physical security, the growing global concerns of business security, and the role people play in making business security a success.

I am grateful to the many experts who took time from their busy lives to contribute to this project. They embraced it and realized the importance of sharing what they know with others to help improve business security. Hopefully, readers will benefit from the information compiled in these two volumes and use it to make their workplaces safer.

Volume 1: *Securing the Enterprise*

The workplace is very different than it was just ten years ago. Computers and the Internet have become common business tools. The tragic events of 9/11 still resonate in organizations, as terrorism remains a concern. Corporate misdeeds from Enron, Tyco, and others have resulted in new regulations, creating renewed interest in business ethics. This changing workplace environment requires revisions in how we approach business security. The entries in Volume 1: *Securing the Enterprise* reflect this evolving workplace.

Volume 1 begins with the Information (Cyber) Protection section. While computers and the Internet increase business productivity, they also create enormous security risks. Protecting data and access to a computer system must be a priority for all organizations and a concern that all employees share. The entries reflect the range of issues and concerns that emerge as information security grows in importance. This section starts with a general discussion of information security and then moves to core concepts in information security:

- Security models
- Security documentation
- Security policies and standards

These core concepts are followed by a collection of additional information security concerns including the security threats and ways to protect Internet and e-mail use, portable device use, insider threat, and social engineering.

Terrorism is a reality that organizations face all around the globe and is broader than most people might think. The Terrorism as a Business Security and Safety Concern section begins with an analysis of terrorism including the global locations at greatest risk. The entry Ecoterrorism reflects the broad nature of terrorism. The breadth and scope of terrorism have implications for business security. Organizations anywhere, for example, might have to deal with environmental groups targeting a facility. Another feature of this section is its consideration of special terrorist risks for agriculture (Agroterrorism, Strategic Partnership Program Agroterrorism, and Food Security) and the chemical industry (Terrorism and Chemical Facilities). Both industries are prime terror targets and need to address terror concerns as part of business security.

The General Safety Concerns section relates to the connections between security and safety. This section examines the role of business security in protecting people and things both inside and outside of the organization. Efforts to protect employees and others in and around an organization must address the concerns generated by significant negative events such as disasters, crises, emergencies, and business disruptions. These negative events are often interconnected and can be threats inside and outside of the organization. The entries cover these important areas:

- Emergency preparedness and response component
- Disaster recovery management
- Business continuity
- Crisis management

Preparations for these negative events are a key to safety, and security can contribute significantly to these efforts. These entries concentrate on crisis management and emergency management because of the strong focus these two processes have on protecting people.

Finally the Uncommon Business Security Concerns section reflects the growing concern over ethics in organizations (Ethics as a Business Security Concern and Ethical Conduct Audit) and the issues of corruption (Corruption as a Business Security Concern) that arise as organizations compete in a global business environment. Ethical and corruption issues do relate to business security. Competitive intelligence is included because organizations can step over the ethical line when seeking competitive intelligence and should know how to make it more difficult for others to collect intelligence on them. The final entry, Reputation Management, is included because many other entries note the negative effect that security lapses can have on an organization's reputation. This entry explains why damage to a reputation is such a strong business concern.

Volume 2: *Securing People and Processes*

As the workplace changes, the core need for physical protection remains but its nature changes as well. The Physical Protection section contains a variety of entries related to protecting people, equipment, and buildings. The main topics include the following:

- Security guards/officers
- Workplace violence
- Employee background screening and drug testing
- Video surveillance
- Radio frequency identity
- Biometrics
- Shelter-in-place
- Evacuation

The last entry in this section explains how physical and information security are beginning to merge and what the benefits of that synergy are.

The Security on a Global Scale section recognizes the unique security demands of global organizations. The Terrorism entries touched on the subject, but this section's entries look at the problems and possible security solutions when an organization is connected to various locations around the world. The topics include the following:

- Pandemics
- Outsourcing
- Supply chain security
- Travel overseas
- Corporate or industrial espionage

A theme that echoes throughout this introduction and collection is the importance of all employees in security. The entries in the Enhancing the Human Side of Security and Safety section concentrate on how to work with employees to embrace programs that will make a more secure workplace. The focus is on how to integrate new programs into an organization by avoiding the silo thinking that prevents integration, winning acceptance, and integrating the new programs into the organizational culture. The entries also provide tips on how to create teams and the value of exercises and training.

Volume 2 also includes the Guidance Appendix, Resource Appendix, Documents Appendix, and Glossary. The Guidance Appendix provides "how-to" advice on a number of the topics in the two volumes; whereas the Resource Appendix lists books, magazines, and web sites that can provide additional information on a variety of the entries. The Document Appendix offers a collection of government documents that are useful reference tools for those interested in business security. Last, the Glossary provides an extensive list of terms related to business security. It is a useful tool for clarifying the meaning of terms or concepts and learning the diverse vocabulary of business security.

Business security is a complex topic that involves a wide range of activities and preventative measures. Hopefully the *PSI Handbook of Business Security* does justice to the complicated nature of the topic. Many departments in an organization have a role to play in business security. These two volumes illustrate how the various elements of business security in an organization must work in concert and include all employees in that effort. This project will be a success if people use the ideas in this book to improve security in their organizations.

ACKNOWLEDGMENTS

I would like to thank the many attendees and presenters at CPM West that I have talked to and heard over the years. Your ideas about and insights into business security helped to guide the development of this project. I would also like to thank Jeff Olson at Praeger Publishers, Greenwood Publishing Group, for his dedicated attention to and editing of this project.

INFORMATION (CYBER) PROTECTION

The increased use of computers and the Internet in the workplace raises the need and value of information security. This section examines many of the issues related to information security along with policies and actions that can be taken to improve information security.

INFORMATION SECURITY

W. Timothy Coombs

Businesses cannot operate without computers. Companies are also finding that operations are becoming more involved with the Internet, including wireless networks and portable devices such as cell phones and PDAs. Just as individuals must protect their identities, companies must protect their vital information.

Information security, also known as cyber security, is a term used to describe efforts to prevent, detect, and respond to attacks on a company's information. Breaches in information security hurt an organization in many ways. There are financial losses from destroyed or compromised documents, upset customers who are at risk from information the company has lost, and damages from lawsuits. The company's reputation suffers as well because people have less faith in its ability to safeguard information.

THREATS

Three main threats to cyber security are external attacks, insider attacks, and malicious code. External attacks come from people who use weaknesses in a computer system or software to gain access to a system. Common labels for these attackers are hackers, attackers, and intruders. Although some external attacks are a result of mischief or curiosity, the attacks can be very serious and expensive. The primary concern is your data and information. Data and information can be stolen, destroyed, or altered once an attacker is in your system. Any of these actions can harm your company. Insider attacks are by current or former employees, including contract workers. Insiders know the system and how to access it. As the Insider Threat entry notes, they are the most dangerous threat to information security. Refer to the Insider Threat entry for a detailed discussion of the topic.

Malicious codes include viruses, worms, and Trojan horses. Each of these has slightly different characteristics. Viruses are the codes you hear about the most in the news. To get a virus, you must actually do something that allows the code to infect your computer. A viral infection can be caused by opening an e-mail attachment or visiting a web page. Worms can move through systems without any help from a user. The worm uses weaknesses in software to infect a computer. Worms can also be spread via e-mail and web sites but are self-propagating. A Trojan horse is software that pretends to be something else. It claims to do one thing but performs other nefarious operations in the background. The program may claim to allow file sharing when it is really allowing an attacker to enter and search your computer files. Understanding these cyber threats helps organizations prepare for cyber security.[1]

PREVENTION

The basics of information security are good security habits and proper protective measures. Individuals in your organization need to engage in proper security habits. People should be trained in what these habits are, why they are important, and how to go about executing them. Three simple security habits are locking the computer, checking security settings, and using passwords. Whenever you are using a computer that has secure information, lock the computer when you are away from it. Even a few minutes can give a person time to damage or steal files. If someone is lurking inside your company, he or she can use your computer if you leave it on and open. Refer to the Social Engineering entry for more information about how people enter work areas.

Many software packages, including e-mail and browsers, offer different levels of security. Employees should be encouraged to use the proper level of security setting in the workplace and on any other computers they use for work-related activities. Security settings for a web browser are a common example. Work computers should be set to the highest level possible. The highest security level can result in some web pages not functioning or loading properly. JavaScript or Java and ActiveX controls are used by many web sites but are often blocked by the highest security level. The reason for the block is that attackers can use these functionalities to gain access to a computer. They may download or execute malicious code. Web browsers may use different terms but allow users to define *zones* that apply different security levels to each zone. If employees need to access trusted web sites with these functionalities, the web sites can be added to a list of trusted sites to which a lower level of security can be applied.

The security settings have options for handling cookies and pop-up windows. Companies will want to limit cookies (the collection of information about your computer and web browsing) by blocking or limiting cookies. One method to control cookies is to choose whether to allow a cookie from a web site a person is visiting. It is best always to block cookies from a third party. Pop-ups are another means for attackers to gain access to a computer or a system. Security settings should seek to block pop-up windows. Again, pop-ups affect the functionality of some web sites. Pop-ups can be turned on for safe web sites that require pop-ups for the web site to be viewed and used properly.

Passwords are an important part of cyber security that people often water down because they can be inconvenient. Passwords limit computers to authorized users. It is one form of authentication. Newer biometric authentication can replace passwords for computer access but not access to particular web sites or intranet sites. Passwords take time to type in and people might forget them. The end result is that people select overly simple passwords, allow the computer to remember the password, or write the password on a piece of paper near their computer. Simple passwords are easy to crack; attackers simply guess words or numbers. Good guesses include phone numbers, birthdays, or pets' names. Word-based passwords are vulnerable to dictionary attacks that simply guess words from the dictionary.

Strong passwords include a combination of letters (upper and lower case), special characters, and numbers. But strong passwords are difficult to remember. Some programs allow the computer to remember the password. However, the remembered password is then on the computer and a skilled user can easily find where it is stored and use it. Other times, people write down the password and leave it near the computer. Anyone who has access to the area can find and use the password.

Here are some basic guides for using passwords developed by the US-CERT program and Carnegie Mellon University:

1. Do not use words found in the dictionary, even those from another language.
2. Different systems should have different passwords, not just one.
3. Use upper and lower-case letters.
4. Use a combination of numbers, special characters, and letters.
5. Do not use passwords derived from personal information such as birthdays.
6. Use a mnemonic to help you remember a password.[2]

Protective measures include but are not limited to firewalls, antivirus software, spyware defense, digital signatures, and encryption. Firewalls can be hardware or software designed to protect your computer from attackers. They work by limiting Internet traffic. Hardware is known as network firewalls. This actual device is located between a computer or network and the cable or DSL Internet connection. The advantage of a hardware firewall is that it is a separate device providing the protection as opposed to software loaded into the machine it is designed to protect. Firewalls are not 100 percent effective, so good security habits are still needed.

A number of companies offer antivirus software. Do not download antivirus from web sites because the risk of downloading malicious code instead is too great. Instead install antivirus software from DVDs or CDs. The antivirus software has different security settings, and your company will need to determine the appropriate levels for your users. Antivirus software scans files for infections. An infection is detected by discovering patterns associated with an infection. This means a program can find only viruses it knows. Because new viruses constantly appear, it is critical to update antivirus software regularly. It is recommended to purchase antivirus software that provides regular updates for more effective protection. Again, antivirus software does not guarantee 100 percent protection, so good security habits are still required. A user can scan incoming files or any files on a computer. It is recommended to scan incoming files, such as e-mail attachments, before opening them. It is also a good idea to scan your computer files regularly for any viruses. You can execute the scans manually or automatically.

Spyware or adware is used by advertisers to control material people see when they are online. Spyware can send you pop-ups, redirect your browser to a web site, or track your Internet activities. One indicator a computer has spyware is that it becomes slow or sluggish. The reduced speed is a result of the extra processing it requires. Here is a list of spyware symptoms provided by US-CERT:

1. Endless pop-ups
2. Redirection to web sites other than the ones you selected
3. Appearance of new toolbars on your web browser
4. Appearance of new icons along the bottom of your computer screen
5. The home page of your browser changes
6. Different search engine appears when you click your search icon
7. Certain keys do not work in your browser
8. Appearance of random Window error messages
9. Noticeable drop in your computer's processing speed[3]

Reputable vendors offer software to detect and remove spyware. Some antivirus software provides spyware protections as well. Be careful if you use separate antivirus and antispyware programs. The programs could be incompatible, causing false readings and programs attacking one another. Good security practices help to prevent spyware. Recommendations include not clicking on links in pop-ups, choosing “no” when asked a question in a box on your screen, avoiding free downloadable software, and not following links to free antispyware software. Spyware is another reason employee computers should be set to limit pop-ups and cookies.

Digital signatures and encryption are related ways to increase security for e-mail exchanges. A digital signature provides verification that an e-mail is really from the person claming to have sent it and that the e-mail has not been altered. The digital signature appears as a series of block numbers and letters at the bottom of a message. Although the string appears to be random, it was generated using a mathematical algorithm. The idea is to prevent fake e-mails from being sent in the sender’s name and to ensure the message had arrived intact.

Keys are used to create the digital signature. Each signature has two keys, a private key and a public key. A private key is used by the person sending the e-mail message and is password protected. A public key is made available to the receiver of the message and is used to verify the signature. Public keys can be sent to a person or downloaded from a public key ring. A key ring contains the keys of people who have sent you their keys or that you have downloaded from a public key ring/key server. A public key server is composed of keys people have decided to upload. To confirm a key, the fingerprint is examined. The fingerprint is a series of numbers and letters but not the same ones that appear at the bottom of the message.

To have a digital signature, you need to have software that allows you to create a key. You then upload the key to a public key ring/server. Then when you send a message, the receiver can use the public key ring/server to verify your digital signature. You then need to digitally sign your e-mail messages. Most e-mail systems will provide an option for digital signatures.

Encryption is a coded message that is an excellent choice for sensitive information. Unless people have the key for decoding the message, all they will see is a random series of characters, letters, and numbers. Encryption uses keys as well. When you encrypt a message, you use the recipient’s public key. The receiver then uses his or her private key to decrypt the message. The sender begins by getting the recipient’s public key. Confirm the fingerprint with the recipient. The message is then encrypted using the public key and e-mailed to the recipient. The recipient receives and decrypts the message. Encryption adds an extra layer of security to e-mails. This is important given the risk of people intercepting e-mails, especially on wireless networks.

One other point needs to be made about information security measures: Install patches. Software is not perfect, and it often has vulnerabilities that attackers can exploit. This is how worms can self-generate. When vendors discover a vulnerability, they create patches to fix the problems. Users should install patches as soon as they are available. Some software automatically checks for updates, whereas some vendors send patch notification. However, download patches only from trusted web sites. Downloading patches helps to increase the security shield around a computer.

CONCLUSION

Information security becomes more important with each passing month. Organizations will continue to increase their use of the Internet, including e-mail, and the reliance on computers to store and to move information. Organizations must construct information security policies and work to ensure that all employees follow these policies. Everyone in the organization has a responsibility for information security.

See also Data Backup; Developing, Publishing, and Maintaining Information Security Policies and Standards; Integrating Physical and Information Security; Insider Threat; Internet and E-mail Use Policies; Portable Device Security; Security Documentation; Security Models; Social Engineering: Exploiting the Weakest Link; and US-CERT.

NOTES

1. ICD, “2006 Global Information Security Workforce Study,” October 2006, online at https://www.isc2.org/download/workforcestudy06.pdf (accessed 5 March 2007).

2. CERT, “Protecting Yourself from Password File Attacks,” 24 Sept. 2002, online at http://www.cert.org/tech_tips/passwd_file_protection.html (accessed 28 Jan. 2007).

3. US-CERT, “Recognizing and Avoiding Spyware,” 2004, online at http://www.us-cert.gov/cas/tips/ST04-016.html (accessed 28 Jan. 2007).

SECURITY MODELS

Douglas G. Conorich

A *security model* is a scheme or framework for specifying and enforcing the organization’s security policies. It sets up the requirements necessary to support the organization’s documented security policy. A security model may be founded upon a formal model of access rights, a model of computation, a model of distributed computing, a mixed or combined model, or with no particular theoretical grounding at all.[1] It works hand-in-hand with the security architecture, or the framework of the organization’s system. The requirements document tells an organization how to carry out its security policy.

The purpose of a security model is to provide assurance to organizations. It offers the level of confidence that an organization’s security program is going to protect it. The security model is divided into layers that range from the organization’s business objectives down to the total security of the organization. Each layer provides support for the layer above it and protection for the layer below it. Say the top layer is the business objectives, and the next layer down contains vulnerability assessments and penetration testing. The vulnerability assessments and penetration testing layer then supports the business objectives and protects whatever layer is below it.[2]

UNIQUENESS OF A SECURITY MODEL

Because no two organizations have the same security policy, no two organizations have the same security model. The security model always starts with the organization's business objectives and ends with the organization's total security. It is important to remember that it is the business objectives that drive the security model, and not the security model that drives the business objectives.

Assessing your business model is usually fairly easy. Your organization wants to make money or provide a service. To do this you need to protect your data, trade secrets, processes, and so on. You also have different departments and each of these may have its own business objectives. Therefore, you may want to derive a separate security model for each of the departments. These models define how you provide security for the department's processes and objectives. The organization's security model then provides the framework of how the separate units' models combine and communicate.

Because your business model is time sensitive, your security model must also be time sensitive. You have operational, tactical, and strategic goals that have application in both our business and personal lives. An operational goal can determine how much raw materials my plant needs today to produce its desired number of widgets. In my personal life, what am I having for dinner tonight and do I have to go to the store to prepare for it? Tactical goals are a little farther out. This could be the sales quota for next year for each of my salespeople, or your belief that you are going to need a new car in three years. How will you pay for it? Tactical goals take a lot more planning. What I do today has very little impact on these goals, but it does determine what I need to do tomorrow and the next x number of tomorrows. Strategic goals are long range. Where do I see my organization in three to five years? Will I have enough money to retire at age fifty?

For computer security, operational goals might be how I will access my computer resources or to make sure that my web site can access the data it needs to function properly. A tactical goal could be to develop a scheme to protect my data in motion and my data in static using public key infrastructure (PKI). A strategic goal might be to replace all my Windows servers with hardened Linux servers. Each of these goals provides for security now, how to improve security in the short term, and what your plans are to create an even more secure environment in the more distant future.

The object of this planning is to ensure a smooth transition from operational to tactical to strategic. You want to make sure that what you are doing today will help you install and use what you need tomorrow. The last thing that you want to do is have to rip everything out so you can get to the next step. In the case above, you don’t want to set up an encryption scheme for your data in motion and static protection that works on Windows and not on Linux.

SECURITY PLANNING PROCESS

Security planning needs to take a bottom-up approach. If you were going to build a house, you would first determine what the house would be used for (vacation, hunting, living, etc.). The next step would be to sketch out the requirements (number of bedrooms, size of the kitchen, fireplace, etc.). Then you would want to start drawing a blueprint. Without a blueprint, you would never know what the house would look like when it was done. With security, you need to start the same way. Begin with the goals—the overall goals of the organization, the goals for each of the departments, and the goals of the work units. Now that you know where you want to go, you can start to figure out how to get there. The next step is to determine the processes and the security requirements for each one. These requirements build the framework of your security policy. From your security policy, determine what level of assurance you need; for example, “I need a 100 percent assurance that if an unauthorized person accesses the credit card database, he or she will not be able to read it.” This determines what to put in place to reach that assurance level, that is, firewalls, networks, access controls, and so forth. This is your security model.

SECURE STATE MACHINE MODELS

Several security models depend on the state of the system, which is a point-in-time snapshot of all the permissions and the relationships between subjects and objects. The subject is any entity that requests access. The object is the thing that is requested. A user requesting access to a web server creates a subject and object relationship. The web server requesting credentials from the authentication database also forms a subject and object relationship. The web server can be both an object in the former case and a subject in the latter. Maintaining a secure state for a system requires that all transactions between subjects and objects are in accordance with those restrictions defined by the security policy. State transition actions are those processes that alter the state of the system. Each system has a finite number of transition actions.

In a secure state machine model, you have to enumerate every possible state transition action that can occur. With every conceivable state transition action, you always start with the machine in a secure state and then determine whether you will end up with a secure state after the completion of the state transition action. If you can show that, after every possible state transition action, the machine ends up in a secure state, then you have a secure state machine model.

The first of these secure state machine models is the Bell-LaPadula Model, designed in 1973. David Bell and Len LaPadula developed this model for the Department of Defense (DOD) to address the DOD's concern with its multilevel security (MLS) policy. A multilevel security policy is one in which the computer or database contains information that has different security classifications (top secret, secret, confidential, unclassified). It is applied when users with different security clearances and needs-to-know can simultaneously access the system or database. The object of the policy is to ensure that users do not gain access to information that they are not cleared for. The model focuses on the classification of the object and authorization to access the object. Although this model was designed with the government in mind, it can be used by commercial organizations that have a multilevel security classification system.

The Bell-LaPadula Model is an information-flow security model. It uses subjects, objects, access requests (read, write, both), and security levels to determine whether an operation is within the security policy. Within the Bell-LaPadula Model, the security clearance and the need to know of each subject and the classification of every object are stored in an authentication database. The classifications are organized in a lattice that has an upper bound and a lower bound. In the case of the DOD previously mentioned, the upper bound would be top secret and the lower bound unclassified. The security clearance and the need to know of a subject are compared to the classification of the object, if a request for access is initiated. Access is permitted only if it is in accordance with the stated security policy. In a multilevel security policy, the lattice is used to determine the access. The subject's security clearance and the need to know are used to set the upper bound in the lattice, and then the subject can access that level down to the lower bound of the lattice. As long as the subject's security clearance is equal to or higher than the classification of the object, the security policy is met. Someone with secret clearance could access secret, confidential, and unclassified, but not top Secret materials.

The Bell-LaPadula Model defines security properties around two mandatory access control (MAC) rules and one discretionary access control (DAC) rule. The first is the simple security property, which states that subjects cannot read up. Subjects cannot read an object with a higher classification than their security clearance, as stated above. The next is the *-property (read star property), the no-write-down rule, which states that a subject with a secret classification cannot write into a document with a classification of confidential or unclassified. Users can create documents at or above their security clearance, which ensures that data with a higher classification cannot be transferred to data with a lower classification. The last is the discretionary access property, which defines the access matrix that specifies the discretionary access control: what subjects can access what objects.

The exception to the *-property is for trusted subjects. A trusted subject is one that has proven to be trustworthy, which means that the subject always manually performs functions within the security policy. Trusted subjects can transfer information from a higher-classified object to a lower-classified object. If a data element is classified secret, it may contain both secret and lower-classified data. The overall classification is that of the highest-classified data. The *-property looks at the overall classification when it makes its decision whether the data can be copied. The trusted user can manually override the *-property by evaluating each piece of data and pick a confidential piece from the secret data element and copy it to a confidential data element. The Bell-LaPadula Model trusts the trusted user not to do something that is not in harmony with the security policy.

The Bell-LaPadula Model makes sure that secret data remain secret and private data remain private, but it does have some drawbacks. First, it deals only with confidentiality, not with integrity or availability. The model does not address or inhibit backdoors or other hacking methods such as steganography, MT63, and the like. The Bell-LaPadula Model addresses access to data, but not the management of that access. There is no process to modify access rights. Last, in regard to today's computing environment, it does not address the ability for a computer to do file sharing.

A follow-up to the Bell-LaPadula Model is the Biba Integrity Model. Designed by Ken Biba about four years after the Bell-LaPadula Model, this is also a secure state machine model. The Biba Integrity Model is based on access control rules that ensure data integrity. This model organizes the subjects and objects into groups described by a data integrity level. The subject is restricted from writing to data in a higher data integrity level than its own and cannot be corrupted by data written by a lower level than its own. This model is characterized by the no write up and no read down. If I were going to write an article for the local newspaper on global warming, I could read articles written by world-renowned scientists, but I would not write information I found on conspiracytheory.org. Conversely, the world-renowned scientists would not use my article as proof in their research.

Because the Biba Integrity Model is designed to ensure data integrity, it prevents unauthorized subjects from making modifications to data elements. It maintains the internal and an external consistency to the real world.

The Bell-LaPadula Model was designed for the government, which is more concerned with preventing the leaking of secrets. The Biba Integrity Model is intended more for commercial organizations that have greater concern for the integrity of their data.

The next model, the Clark-Wilson Integrity Model, is derived from a paper written by David Clark and David Wilson in 1987. They designed this model to formalize information integrity, which is maintained by ensuring unauthorized subjects do not corrupt data in error or with malicious intent. This is also a secure state machine model because as a computer moves from one state to another due to any number of transition actions, the data remain valid. The Clark-Wilson Integrity Model defines both certification rules and enforcement rules. David Clark and David Wilson wrote the model specifically for the commercial world, which may be running a multilevel security system.

The Clark-Wilson Integrity Model's certification rules and enforcement rules are based on transactions. A trusted transaction is one that transforms the system from one secure state to another secure state. The basis of the integrity of the system is the integrity of the transaction.

In the Clark-Wilson Integrity Model, subjects cannot access the objects directly. Users must use a program to modify the data, and this additional layer of protection helps to ensure the integrity of the data. Users are given authorization to use only programs they are allowed to use. The programs permit the user to do only certain things. Take the example of an automated teller machine. You, as the user, cannot interact with the data directly; you must use the programs that the machine presents to you. You cannot empty all the money from your account. You can withdraw only $200. By forcing the user to use only preapproved programs that can perform only certain authorized actions, you can keep the data from being changed in an unauthorized manner.

This model also uses the principle of separation of duties, which states that each transaction is divided into a number of smaller transactions. By assigning these transactions to separate individuals to accomplish, a single user is prevented from corrupting data without the collusion of others. A teller cannot perform a transaction amounting to $10,000 or more without the approval of a teller supervisor.

A third piece of the model revolves around auditing. The model requires the tracking of information received from outside the trusted system. By default, all internal data are considered trusted. The key data element, called a constrained data item, is considered trusted by an integrity verification procedure. All transaction procedures must certify that all constrained data items and all unconstrained data items are transformed to security constrained data items. Auditing tracks this process and reports on it.

Another model is the Graham-Denning Model, which addresses those issues involving granting rights to users and how the users can use those rights on objects. Here are eight basic protections it defines:

1. How to securely create for an object
2. How to create for a subject
3. How to securely delete for an object
4. How to securely delete for a subject
5. How to securely grant the read access right
6. How to securely grant the write access right
7. How to securely grant the delete access right
8. How to securely grant the transfer access right

The Graham-Denning Model addresses the management of that access and the process to modify access rights.

The Brewer and Nash Model gives an organization information security access control that can change dynamically. This information-flow model, also known as the Chinese Wall Model, provides controls such that there can be no conflict of interest between the subject and the object. A conflict of interest occurs when a trusted subject has competing professional and personal interests. A conflict of interest does not imply that anything improper or unethical has occurred; just that it will be difficult for the subject to make a completely impartial decision. In many cases, third-party verification is required. If I am responsible for the security of my web site, I cannot impartially verify that it is Payment Card Industry (PCI) compliant. I need to use a certified third-party tool or professional services engagement to do that.

The last model to discuss is the noninterference model, which simply states that transactions at one level of a system do not affect the state of the system at a lower level of the system. If a transaction that has occurred at a level above me changes my state of the system, then I might be able to deduce what that transaction was. Thus information was leaked. If a decision is being made in the boardroom for a merger and memos are released to stop doing certain things, I might figure out that the merger is happening. This could manipulate the stock prices.

CONCLUSION

These are just a few of the many variants of these and other security models. In many cases, organizations do not use only one of these but also may combine the best and most useful parts for their security model. In reality, there is probably a security model for the overall organization and variants or subsets for different departments, depending on their varied needs.

See also Developing, Publishing, and Maintaining Information Security Policies and Standards; Information Security; and Security Documentation.

NOTES

1. "Computer Security Model," 21 April 2007, online at http://en.wikipedia.org/wiki/Computer_security_model (accessed 23 April 2007).

2. Shon Harris, *CISSP All-in-One Certification Exam Guide*, 3rd ed. (Columbus, OH: McGraw Hill/Osborne, 2005).

SECURITY DOCUMENTATION

Douglas G. Conorich

Documentation has become both the boon and the bane of any security program. As the old adage states, "Nothing is ever complete until the documentation is done." Senior management is responsible for security documentation. This documentation needs to define the scope of security in the organization and to determine what is to be protected and to what extent. It also explains what is expected from employees and what the consequences are of noncompliance. Security documentation falls into four categories: goals, requirements, steps, and proof.

The purpose of security documentation is to show both due care and due diligence. These are both legal terms that determine whether a company or individual can be held liable for some event. In security, *due care* is the care that a reasonable person or company would exercise to secure its data. It defines your legal duty. It shows that a company has taken responsibility for its activities and taken the necessary steps to help protect itself and its assets from possible risks. *Due diligence* is a term used to determine whether due care has actually occurred.[1] Activities that make sure the protection mechanisms are continually used, maintained, and operational are evidence of due diligence. In practice, do I have the rules and procedures in place to secure my data, and can I prove that I am actually doing it?

CREATING SECURITY DOCUMENTATION

Security documentation starts with the creation of an organization security policy, which should outline the goals of your organization, what is and is not allowed, and the consequences. It determines the policies, procedures, baselines, and guidelines to accomplish security, and what you will need to prove that you have done it. It delineates how data will be managed, stored, protected, destroyed, and moved. The security requirements of your organization build the framework around which you write your security policy.

The first objective in writing an information security policy is to investigate the requirements for information security and the associated priorities. You then can develop the custom policies and standards necessary to safeguard the organization's information assets. To do this, you must take into account the common requirements to all organizations—contractual, business continuity, and protection aspects—and then consider the requirements unique to your organization—regulations, type of business, and your organization's business culture.

Let us start with a few definitions:

- *Policies.* These management instructions indicate how an organization is to be run. They are high-level statements of goals, objectives, beliefs, ethics, and responsibilities. Compliance to corporate policy is mandatory, and special approval is required should an individual wish to take a contrary course of action.

- *Standard.* These are sets of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures, and other detail factors. Compliance with standards is required.
- *Process.* Processes are activities, tasks, and procedures typically performed across multiple organizations to implement company policies and standards.
- *Procedures.* These are specific operational steps that individuals must take to achieve goals that are often stated in policies.
- *Baseline.* The minimum level of assurance that you can have is your baseline.
- *Guidelines.* These sets of procedures are like standards, except that they are recommendations, instead of being mandatory.

GOALS

Goals are an important part of any program. Without a goal in mind, you will end up where you are heading. This may be, but most likely not, where you want to be. Your goal should be stated as a mission statement from the top executive of your organization. You should have mission statements for your company, each division, and even down to each department. The lower in the food chain you are in the organization, the more specific the statement can become. Security needs to be identified as a business enabler and not as an inhibitor.

An example of an organization mission statement related to security follows:

> This company has a large variety of assets. Many are of great value to (*company name*)'s competitiveness and success as a business. They include our physical assets and our extremely valuable proprietary information, such as (*company name*)'s intellectual property and (*company name*)'s confidential information. Protecting all of these assets is critical. Their loss, theft, or misuse jeopardizes the future of (*company name*). You are personally responsible for protecting (*company name*)'s property entrusted to you and for helping to protect the company's assets in general. To do this, you should be aware of and understand (*company name*)'s security procedures. You need to be alert to any situations or incidents that could lead to the loss, misuse, or theft of company property. You should report all such situations to the security department or your manager as soon as they come to your attention. Ignoring (*company name*)'s security procedures will have consequences that may, in certain instances, lead to termination of your employment.

REQUIREMENTS

If you want to start a bank, the first thing necessary is to ensure that it is against the law to steal the money. If it isn't, then there are no consequences to stop people from trying to steal it. So of primary use in your security program are rules. Rules are important, because they determine what can be done, what specifically cannot be done, how you can make exceptions, and what the consequences are for breaking the rules. The rules not only set down the law but also

- Set the tone of management
- Establish roles and responsibilities
- Define asset classifications
- Provide direction for decisions
- Establish scope of authority
- Provide a basis for procedures
- Establish accountability
- Describe appropriate use of assets
- Establish relationship to legal requirements

When it comes to making rules, you must understand that if you do not specify that something is *not* allowed, then someone will imply that it is. One of the biggest problems companies have faced over the last several years is sexual harassment, including the viewing of pornographic web sites, and online gaming. Companies need to enumerate how employees will use company telephones, e-mail, and Internet access and what inappropriate use is.

Another point of contention between companies and their employees is their right to privacy. Employees need to know and understand that employers have the right to monitor and audit e-mail and telephone communications owned by the company.

An example of a privacy policy follows:

> Personal items, messages, or information that you consider private should not be placed or kept anywhere in the (*company name*) workplace, such as in telephone systems, office systems, electronic files, desks, credenzas, lockers, or offices. (*company name*)'s management has the right to access those areas and any other (*company name*) furnished facilities. Additionally, in order to protect its employees and assets, (*company name*) may ask to search an employee's personal property, including briefcases and bags, located on or being removed from (*company name*) locations; the employee is expected to cooperate with such a request. Employees should not access another employee's work space, including electronic files, without prior approval from management.

STEPS

Goals and requirements are determined by policies and standards. A policy sets direction. A standard is associated with the implementation that follows the path that has been set by that policy. Procedures are the steps to take to meet the goals and standards. The documentation that determines the steps that will accomplish this may be policies, standards, baselines, processes, procedures, and guidelines.

PROOF

It is very nice to say, "This is what I want to do, these are the rules I have set up for my employees to follow, and these are the processes and procedures that I have in place. Ultimately, I am going to have to prove that all this has been done and I really am securing my data." Everything boils down to—can you prove it? You need to show not only that you have done it but also that you have done something with it. If you only identify that your system needs a particular patch to the operating system, then don't apply the patch, you have not improved your security and thus you cannot prove due diligence. As an example, let's take a company's adherence to Sarbanes–Oxley, Section 404: Management Assessment of Internal Controls. The law states:

> Requires each annual report of an issuer to contain an "internal control report," which shall:
>
> (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
> (2) contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

To meet the requirements of the law, the policy statement could be appended with:

> (*company name*) will take all necessary steps to comply with the Sarbanes-Oxley Act.

This statement meets the definition of a goal at the executive level. It clearly implies what the company is aiming for and does not specify the how.

The requirements must now define how to carry out the new rules implementing Section 404 of the act. The company may define the term *internal control over financial reporting* to mean provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the registrant's assets that could have a material effect on the financial statements. It also needs to specify the roles and responsibilities in carrying out this requirement. In this case, the company assigns responsibility to the chief security officer for ensuring that steps are in place to monitor for vulnerabilities and intrusions. The director of information technology (IT) would consequently be responsible for establishing safeguards for your organization, that is, a vulnerability management and an intrusion detection/prevention (IDS/IPS) program.

An example of a requirement could be the following:

> The importance of implementing a best practices methodology for addressing vulnerabilities and intrusions is becoming increasingly apparent in light of the pressures of regulatory compliance. (*company name*) needs to develop a vulnerability management and an intrusion prevention program that is designed to help expedite implementation of the tools, methodologies, and best practices required to address today's dynamic vulnerability and threat landscape. By combining internal and external managed scanning services with practiced work flow and case management capabilities, organizations can receive comprehensive visibility into each area of potential exposure within a distributed network environment.

Enumerating the processes, procedures, guidelines, and baselines is a lot more verbose a step. For both the vulnerability management and intrusion detection/prevention programs, the company must determine the how, what, where, and when each will be carried out.

VULNERABILITY MANAGEMENT

It is vital to design vulnerability management to provide the organization with a solution that focuses not only on vulnerability discovery but also on prioritization, remediation, verification, and customizable reporting. Each of these components forms an integral part of the vulnerability management framework, resulting in risk reduction and effective quantification of overall security posture.

Vulnerability Discovery

The process for vulnerability discovery involves the procurement, placement, and scheduling of a vulnerability scanning tool. Companies may have to buy a service or use a managed security service provider (MSSP) to perform external scanning to gain the look and feel that a hacker may have.

The procedure documentation provides the users of the tool with the appropriate scan policy and frequency. An organization may either have one policy that fits all or have a group of different policies to be run for specific purposes. A company may want to run separate scans to determine operating systems and services, run checks for Windows service pack levels, scan desktops for high- and medium-risk vulnerabilities, and scan web servers for high- and medium-risk vulnerabilities.

Prioritization

An organization procedure catalogs each scanned device (asset) and then assigns business criticality ratings as well as system owners to specific assets. Such data facilitate the notification of asset owners when vulnerabilities are discovered and also the establishment of a personalized view into overall program impacts on security posture. The use of this data as well as the data from the vulnerability discovery process allows organizations to use the common vulnerability scoring system (CVSS).

Remediation

The remediation process enumerates how to assign discovered vulnerabilities to designated asset owners for review and remediation. Such a capability requires the use of some type of ticketing system to facilitate a detailed work flow. Individual asset owners can use the ticketing system as a tool for learning about a specific vulnerability and tracking its remediation within the enterprise.

Verification

The responsibility for vulnerability remediation does not end when an asset owner indicates that he or she has effectively patched a vulnerable application or system. A process needs to address how to check remediated vulnerabilities in subsequent scans and how to then document them as closed.

Customizable Reporting

Detailed procedures must identify what types of reports will be generated and when. More details will be discussed later.

Determining the how, what, and where of IDS/IPS is a little more difficult. IDS/IPS is effective wherever you place it, but these devices and their monitoring and management are expensive. Organizations need to determine their risk and assess the criticality of network segments and servers so they can place IDS/IPS in the most cost-effective manner.

Documentation for the IDS/IPS needs to specify where the IDS/IPS devices/software is to be located and to whom it will report. This documentation contains the priority of the placement and the justification for each device/software. This will help later when the company is compiling its statements of proof.

The main process to create with IDS/IPS is how it is to be monitored. Organizations need to have procedures for building and staffing their security operations center, for escalation of suspicious events, and on how to document incidents. These types of documentation can include standard operating procedures, checklists, training manuals, certifications procedures, and correlation and data mining techniques.

The security documentation that proves what you have done is paramount. Everything to this point is just words. It does not matter what you say you will do and even if you do it; if you cannot prove that you did it, you might as well not have done it. This is done through the creation of reports. A set of your procedures must delineate how you create reports so that they are standardized.

Vulnerability management reporting should provide a results-oriented view into service performance and security posture in either a stand-alone presentation or combined with data from multiple services. Such capabilities allow organizations to articulate effectively the value of a point-specific service or the complete MSSP solution. When combined with customized data sets, user-defined introductions/conclusions, and multiple report views (line level, auditor, manager), organizations can generate reports that speak to technical, as well as business-minded, individuals.

These reports must not only show what vulnerabilities your organization has found but also show an improvement in your security posture. To do this, you could use a ticketing system to indicate who is responsible for correcting the vulnerabilities and what the deadlines are for the responsible person to correct the problem. A good standard is twenty-four hours for a high-risk vulnerability, one week for a medium-risk vulnerability, and thirty days for a low-risk vulnerability.

The necessary reports indicate that you are regularly scanning your systems for vulnerabilities. You also need to have reporting that shows your remediation trend. This report shows the total number of vulnerabilities, the net new vulnerabilities, and how long it takes you to remediate vulnerabilities. How you prove that the vulnerabilities are really gone is also important.

With IDS/IPS you need to demonstrate that you are monitoring. For IDS, report on identified malicious activity and network misuse through passive monitoring of network segments. For IPS, report on active blocking of malicious activity. For both, keep detailed incident-based reports and provide actionable information following each escalation. Such documentation proves due diligence for regulatory compliance. It is crucial to keep an extended log archival. If you are ever sued for a security breach, you may have to retrieve the actual logs for a specified period of time.

CONCLUSION

Security documentation is important at every level of the security model. This documentation serves as the guide to where organizations want to go, what is required, how they will get there, and how can they prove they did what they said they would. Because security is very fluid, this documentation needs to be a living entity. How you change the documentation must be regulated and set to be reviewed on a regular basis. How often depends on your corporate culture and the perceived threat and risk.

See also Developing, Publishing, and Maintaining Information Security Policies and Standards; Information Security; and Security Models.

DEVELOPING, PUBLISHING, AND MAINTAINING INFORMATION SECURITY POLICIES AND STANDARDS

Michael Seese

Mention "information security" and most people think of either the "fancy" devices they read about—such as firewalls, intrusion detection systems, and fingerprint readers—or the more common tools they use every day, such as passwords and access cards. Security policies probably do not immediately come to mind. And yet it is policies that enable the aforementioned technologies to be implemented in the real world. For it is a policy that states that firewalls must be installed along the organization's network perimeter. It is a policy that mandates that passwords be eight characters long and changed every sixty days. Indeed, it is a policy that states that management sees security as a necessary business driver and, as such, that all employees must read and understand the information security policy manual and adhere to its dictates.

Policies form the basis of an organization's entire information security program, which provides a high-level road map for overall security. Policies as guiding principles establish management's authority—and responsibility—to create a secure business environment; outline acceptable and unacceptable behaviors and activities; and present specific direction that drives to a basic goal: the protection of the organization's people, facilities, physical assets, and information assets.

POLICIES, STANDARDS, GUIDELINES, AND PROCEDURES

The term *policy* itself has many applications in the information security arena. For example, you can refer to the security policy on a firewall. However, for the purposes of this article, a policy is a "formal statement of rules by which people who are given access to an organization's technology and information assets must abide."[1] Put into other words, a policy explains what someone should or should not do.

Although the term *policy* often is broadly used to refer to any and all directives, in reality several different types of guiding documents exist that vary primarily in terms of scope and (inversely) life span. Although the terms and definitions may differ, your organization also may make use of standards, guidelines, and procedures.

Policies are broad, high-level documents, covering a range of topics. In short, anything that management wants to regulate can be put into a policy. And although policies should be written to a sufficient level of detail so as to be useful, they should not delve into technological specifics at a level that could quickly make them obsolete. Three to five years is a sensible life span for a policy, though calling for a yearly review for relevance and necessary updates would not be unreasonable. Note that any major organizational changes—such as an acquisition, entering into a new line of business, or the need to comply with recent government mandates—also could prompt a complete, in-depth policy review.

Standards are more issue specific, usually are focused on one technology, and have a shorter life span. A yearly review of all of your security standards would be a sound practice. Whereas each policy does not necessarily require an accompanying standard, each standard should refer to a specific policy. In fact, policies that cover a broad topic—such as user access management—might have multiple standards that support them. For example, your organization might have an "Encryption Policy," which includes language such as "All confidential materials must be encrypted using a method approved by the information security department before being sent to an external e-mail address or physically removed from the company's premises." The attendant "Acceptable Encryption Technologies Standard" would have language such as "Approved encryption technologies include RSA, with a key length of at least 128 bits." That way, if in two years best practice dictates a stronger key, the policy is still valid, while the standard probably already will have been reviewed and revised. Similarly, supporting the encryption policy might be the "Acceptable Laptop Encryption Technologies Standard."

Closely related to standards are *baselines*, or *minimum security baselines* (MSBs). MSBs are operating-system specific and provide extensive and minute detail of OS configuration settings. So, for example, a Windows MSB might specify:

• Password history:	4
• Maximum password age:	60 days
• Minimum password age:	1 day
• Do not display last user name:	Enabled
• Account lockout:	3 invalid attempts

MSBs often are not for "public consumption," because a malicious use could exploit much of the information they contain—especially information related to "guest" and "admin" accounts. If there is a need to provide end users with *some* of the settings, you can pull the requisite information into a standard.

Guidelines are written to the same level of technical detail as standards. The difference is, whereas policies and standards can be thought of as mandates and feature phrases that begin "Users must" and "Users cannot," guidelines are suggestions and indicate what users "should" do. For example, you may have "Secure Coding Guidelines." Although this document may contain the sentence, "Users must employ recognized best coding practices at all times," it is not practical to say, "Error messages *must* not reveal implementation details such as error codes." A developer may have a legitimate need to provide such information. Instead, guidelines must explain why a specific practice may introduce a vulnerability and suggest ways to avoid that unsecure practice.

Procedures are documents that provide the step-by-step instructions necessary to reach a desired end state. Whereas a dedicated documentation specialist—with input from subject matter experts, of course—could write policies, standards, and guidelines, the technical specialist who performs some task on a daily basis would probably write a procedures document. A procedures document entitled "Setting Firewall Access Control Lists" would describe the specific steps that a firewall team technician should follow to set the firewall rules. In that way, if your organization chooses to make "Deny all" (which means, "Deny all traffic that has not been explicitly allowed") the final rule in the set, anyone creating a firewall rule set would know exactly what is expected. Procedures, like MSBs, most likely are not for public consumption, because they contain information that could be used to compromise security.

POLICY STRUCTURE

Although it may seem like a trivial decision, one consideration is whether to maintain the individual policies in stand-alone documents or to compile them into an all-inclusive manual. Both options offer advantages and disadvantages. Separate documents are easier to update, are simpler to reorganize or rearrange, and allow users to print out only the sections they need to reference. On the other hand, a policy manual is easier to print out in total, can be indexed for searching, and can contain a universal glossary. Maintaining individual policies and a compiled manual offers the advantages of both, although it requires more work, as updates to any single policy also must be made to that section of the manual. A document management system (or a content management system) can ease this task.

A document management system offers a number of advantages above and beyond ease of updating. It also can track a document's versioning/history, maintaining a record of revisions that could prove crucial if it were necessary to verify when a specific requirement of a policy took effect. A document management system also helps with archiving, retention, distribution, and work flow.

An organization that chooses not to invest in a document management system probably would find it easiest to maintain the documents in the format of the word processing program used to develop them. However, if the documents were to be published electronically—to the corporate intranet, for example—converting them to a format that could not be easily altered would be a sound security practice. Although the possibility is remote, a policy published in a manner that would allow anyone to modify it could be changed, distributed, and touted as "gospel." A user who followed this adulterated version might introduce unexpected—and unintended—vulnerabilities.

Although the corporate intranet is an ideal vehicle for putting the policy manual into users' hands, in many cases hard copies—though harder to keep current—may be necessary.

POLICY ORGANIZATION

Policies should be organized and grouped logically. One possible scheme would simply be to list them alphabetically. Although sensible on the surface, this arrangement could bog down users, who probably would look for the encryption policy under "E," not realizing it's filed under "A" for "Acceptable Encryption." A better option would be to organize policies according to the guidance of a recognized standard. Some of the more well-known organizational frameworks include Control Objectives for Information and related Technology, or COBIT (http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981); Basel II (http://www.bis.org/publ/bcbsca.htm); and the International Standard for Information Technology—Code of Practice for Information Security Management, also known as ISO/IEC 17799 (http://www.iso.org/iso/en/CatalogueDetailPage. CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=).

A third possible organizational scheme would be to group your policies and standards hierarchically. The first "tier" would be the overall, organizational policies, such as those that define your organization's security program, information security roles, security reviews of third parties, information asset classification, security awareness, change control, separation of duties, incident response, regulatory compliance, and intellectual property rights. Another group of policies would be those that the average end user should know: acceptable use, information labeling and handling, e-mail, user access/passwords, virus prevention, and physical access. The final major block of policies would be those more technical in nature: wireless devices, test environment management, backup and disaster recovery, network management, disposal of electronic media, system requirements, cryptographic controls, and software controls. Even though the majority of your employees will not rely on the technical policies, they nonetheless should be required to read them—or be exposed to them via training—so as to remove the "I didn't know" excuse.

POLICY CONTENT

Your policies should present a consistent look and tone. Consistency improves the reader's level of comfort, because he or she knows where to find specific details. Your organizational needs determine the sections to include in each policy. Here is a suggested list, many of which could appear in the document's header.

Title

A concise title provides users with a clear understanding of the policy's contents. "Acceptable Use," "Wireless Devices," and "E-mail" are good titles; "Accessing External Networks and Personal E-mail from the Corporate Intranet" is not.

However, standards and guidelines may have lengthier titles, because each focuses on a more specific topic.

Version

A consistent numbering system helps users (and the document's author) determine at a glance whether a policy has been updated. If most of the policies in the manual have a version number of 1.0, then a policy with a version of 1.1 has undergone a minor revision, whereas 2.0 represents a major revision.

Last Review Date

This is the date that your organization's subject matter experts most recently reviewed the policy, whether they suggested any changes or not.

Publication Date

This is the date that the policy was most recently published, in either hardcopy or electronic format. If the review-to-publication cycle is short, the publication date probably can be combined with the last review date. Although it may seem trivial, the publication date is an important piece of information to include, because it establishes when the policy took effect and, by extension, the date on which your users became responsible for adhering to it.

Expiration Date

On this specified date the policy will expire. However, if your organization has a defined, regular cycle of reviewing and rewriting all policies, then an individual expiration date probably is not necessary.

Classification

A categorization of the policy document within your organization's overall document classification scheme is helpful. In other words, can the manual be released outside of your organization, or is it for internal use only?

Owner

This party within your organization is responsible for reviewing, revising, and enforcing each policy. More likely than not, the information security department will own most, if not every, policy in its manual. Still, it is possible that certain individual policies could be the responsibility of another department, such as the business contingency planning or risk management group.

ISO Reference

This is the section of the ISO standard (or any other recognized standard) on which the policy is based.

Associated Standards

A list of all standards and guidelines that reference the policy is helpful. Although there is an understandable benefit to cataloging the standards that support each policy, this practice would require the policy to be updated whenever a new standard were added. A better solution would be to have language in each standard or guideline that states, "This standard supports policy X."

Scope

This is to whom the policy applies. Most likely, all employees, contractors, and business partners will be expected to follow all policies. Still, certain policies could apply exclusively to employees or to contractors.

Reporting Violations

There should be a method—or several methods—that your organization's members can use to report a suspected violation of policy. Common reporting avenues include a dedicated e-mail box, a phone number, and a physical mailbox. The latter allows for non-trackable, anonymous complaints, which might be the only avenue that some employees feel comfortable using.

Noncompliance/Penalties

This is a clear statement that explains the repercussions of violating the policy. Termination, termination of contract (for contractors), prosecution, and litigation are all penalties that your organization may consider for violations.

Terms and Definitions

These are any technical, unique, or ambiguous terms used in the policy. One logical place for terms and definitions is within the policy that references the term. However, putting them within the policy could result in multiple occurrences of each. As such, compiling all terms and definitions into a single glossary might be a more sensible approach.

Body

The topic covered determines the length of the real "meat" of the policy. A policy on prohibition of cameras might necessitate only several paragraphs; acceptable use and e-mail policies would likely be longer.

Some of the sections common to all policies—such as classification, reporting violations, and noncompliance/penalties—could be placed in a "preamble" so that they only appear once in an all-inclusive manual. This strategy eliminates redundancy and therefore shortens the manual's overall length. The downside is that any sections pulled from the overall manual are now incomplete.

DEVELOPING SECURITY POLICIES

Developing information security policies is definitely not a one-person effort. Although one individual—ideally an experienced writer, as opposed to a technical staff member—may be the author, that person cannot operate in a vacuum. The author should consult, at minimum, representatives from each group within the information security department and quite likely a number of professionals from other areas of the organization. The information security group provides the subject matter experts who address the salient points of their specific technological competencies—account creation, firewall rules, and wireless, for example—while those from other areas can tackle broader corporate issues, such as human resources, legal, and regulatory compliance. Additionally, the author should consult with representatives from the various operating units so as to ensure that the policies mesh with their business needs. If your policies interfere with a department's functions, the end users *will* find a way to circumvent them. Additionally, if individuals from a range of business units are involved in the creation process, they will see themselves as stakeholders of the policy and be more likely to serve as advocates among their peers.

The first decision is what policies your organization needs. As touched upon in the Policy Organization section, there are certain policies that all entities need: the security program, information security roles, information asset classification, security awareness, separation of duties, acceptable use, information labeling and handling, e-mail, user access/passwords, virus prevention, and physical access. Organizations bound by government or industry regulations want policies that outline the steps necessary for compliance. Beyond that, determining which policies your organization requires involves investigation, discussion, a review of recent audits, and perhaps a risk assessment.

The nature of the business is one determining factor. An organization that performs sensitive operations at its facilities may need to include prohibitions against photography and tours; otherwise, a policy on access controls may be the only physical security guidance necessary. Similarly, a smaller enterprise—with an even smaller IT department—may not need separate policies for change management, network segregation, software controls, and test environment management. Finally, if your organization has no Internet presence, then policies for web page controls and online services will not be needed.

When trying to determine what constitutes a "necessary" policy, consider the various constituencies within your organization. First and foremost is upper management. These managers are concerned with the company's bottom line—which in no way should be seen as an indictment but simply as a reflection of the reality that they are beholden to the company's shareholders. Therefore, anything that interferes with the corporation's ability to do business will not garner their support. However, upper management also must concern itself with ensuring that the organization does not suffer any negative impacts through negligence or failure to adhere to government regulations. A final word about upper management: If it doesn't truly support the policies—or better said, information security itself—then that attitude *will* trickle down through the organization.

Stepping down the management chain, the line of business managers also wants policies that do not interfere with its subordinates' ability to meet their performance goals. However, this group also needs clear-cut guidance to counsel and, if necessary, discipline its staff.

The technical users, such as system and database administrators, actually implement most of the technical policies. Therefore, they require clear, specific directives.

Finally, the end users represent the largest organizational constituency. They view the policies as either a positive or a negative. If the policies are simple, direct, and reasonable—after all, they are not children, but adults—then they will adhere to the policies. It is when policies seem overly restrictive, impractical, and illogical that they rebel. When a technological control is available to enforce the policy—such as a system-required password change—the end users' attitude toward the policy may be less relevant. However, because many of a policy's dictates do not have a corresponding automatic control, user buy-in is essential.

Unfortunately, there is no simple, "one-size-fits-all" way to decide which—or even how many—security policies an organization needs. One major consideration is the amount of governmental regulation covering the industry. Clearly, a financial institution requires more, and more detailed, policies than a restaurant. The size of your organization is another determining factor. An operation that is so small that employees know they can literally pick up the phone and call the compliance officer may need fewer policies, because users can get direct consultation and guidance. Similarly, if the staff is highly technical, the policies can state only high-level, basic requirements and then list specifically prohibited activities. Employees then are expected to exercise good judgment.

Geographical dispersal is another consideration. An organization that operates in a smaller footprint, such as a single city or state, most likely has fewer policies than a similar business that operates in multiple countries. In this scenario, your organization may have a set of high-level policies that explain its overall philosophy and goals, and then site-specific policies to address local concerns. The company's structure also should be taken into account. Although (to say it once more) an organization must have high-level policies that state the overall information security goals, a decentralized organization can task local management with developing additional policies. For example, if user IDs are not managed by a central information security group, then account and password policies may be a local decision . . . though it never hurts to list what is considered best practice. On the other hand, if all user accounts—including those for individual applications—are maintained by a central group using a sufficient robust system, then there may not be a need to have account and password policies. The information security group can decide what constitutes a strong password and an acceptable password life span, and the technology will implement it.

A good source to consult is the SANS Institute, which offers guidance under the SANS Security Policy Project (http://www.sans.org/resources/policies/). This site provides a good overview of security policies, standards, and guidelines, and offers a variety of policy templates that may be downloaded and customized by replacing Company Name with the name of your organization.

The publication of a new policy manual should be accompanied by an awareness/education campaign. If the new manual represents a significant change from the previous version, it is likely that all employees will be affected at some level. Indeed, some may find that what used to be a “standard operating procedure” is now a prohibited activity. Further, because technology is constantly changing, a major revision almost certainly will have policies to deal with technologies that did not even exist (or at least were not common to the corporate world) in the previous version.

EXCEPTIONS TO POLICY

In an ideal world, there would be no variation from the mandates of your security policy. Unfortunately, reality is not so perfect. In many cases, there is a sound business reason for not adhering to a policy. For example, your organization may rely on an old mainframe application that was written before security was a primary concern and, as such, only allows for passwords of four characters, as opposed to the eight characters dictated by policy. In other cases, the justification is weaker, though still important in someone’s eyes. For example, the marketing group wants the locking screen saver disabled so that group members don’t have to worry about jiggling the mouse to maintain a running slide show while conversing with clients at a conference.

In order to sort out the “must haves” from the “nice to haves,” your organization needs to establish a process for reviewing exceptions to its policies and standards.

The first step in your exceptions process must be user education—which is a topic unto itself. After all, if your employees do not *know* that modems or nonstandard PCs are against policy, then how could they be expected to request an exception to policy? Aside from end-user knowledge, two other groups are instrumental in the effort to uncover exceptions. Your organization’s audit department should be sufficiently familiar with policy to be able to recognize violations when reviewing each department’s processes and procedures. Also, your information security department should work closely with the group that manages new projects. Having a security analyst involved from the beginning can help the project team with vetting third parties, choosing applications that offer the most security out-of-the box, and perhaps “encouraging” vendors to synchronize their security settings with the requirements of your organization’s security policies.

Persons requesting exceptions to policy should complete and submit a form that specifies the following:

- The specific policy that their request violates
- An explanation of what they are requesting, including how it violates policy
- A thorough description of their business process, including details of how the policy interferes with their operations

- A business justification
- The impact to their operations if the exception were not granted
- A list of the alternatives considered, and why they were determined to be unacceptable
- A risk assessment, including:
  - The type of data being put at risk
  - Any exposures created if the exception were granted
  - The likelihood that any given vulnerability could be exploited
  - A description of what an attacker could do if he or she exploited the vulnerability created by the exception
  - The impacts to the organization if the vulnerability were exploited
  - Any controls that will be implemented to mitigate the risks

A responsible party in the line of business should sign the form, acknowledging an understanding that the request is putting the organization's information assets at risk.

Requests for exception then should be reviewed. Once again, the size of your organization and your information security department determines whether all or a dedicated subset of the team will review it, and the review format and frequency. If one request per month is submitted, then an ad hoc meeting—or even a simple distribution via e-mail—may be enough. Otherwise, you should have regularly scheduled meetings so that the user community can be made aware of deadlines for submitting requests.

Another consideration is whether to invite applicants to the review meeting. On the one hand, the applicant will be able to answer any technical question that the exception review committee has. However, the committee's discussion may include technical security details that are beyond the average user's "need to know." A well-designed (and fully completed) form goes a long way toward eliminating the need to include the applicant in the discussion.

The committee should carefully consider the duration of the exception. Some requests will have a built-in expiration date: "This exception is needed until the application vendor provides a new release that will remediate the issue, which is expected in the fourth quarter of this year." Other requests may be for an exception "in perpetuity," as in the case of a critical legacy system that will never be modified to meet modern security standards. Even in the latter case, the exception should not be permanent, as someday a fix may be made available. One year is a reasonable maximum for any exception.

Following the meeting, the committee chair should return the form with the committee's decision. A simple approval may need no further explanation. However, the committee may decide to impose one or more conditions on the approval, such as the implementation of compensating managerial controls. A denial certainly needs to include the reason for rejection. If the applicant knows why the request was rejected, he or she may be able to suggest additional controls that answer the committee's concerns. And if the request is escalated, a well-explained reason for the rejection enables the higher-up getting the angry phone call to understand and support the committee's decision.

MAKING A POLICY MANUAL USABLE

By now, it should be obvious why every organization that conducts some manner of business needs a thorough, detailed security policy manual. Your management, technical staff, and end users require guidance in order to adhere to security best practices. And—as harsh as it may seem—policies also provide management with the leverage it needs to discipline employees who fail to follow them. As mentioned above, however, your average user probably does not care about—and truly, on a daily basis, probably does not need to know about—most of your organization's policies. Further, this user probably doesn't want to wade through a 150-page manual that at times reads like a legal brief. As such, there is something to be said for the concept of "less is more."

What is needed is an abridged, simplified manual that tells users what they must know in order to do their jobs securely. Whether you call it the "Abridged Security Policy Manual" or the "Security Policy Manual Lite" is immaterial. What is important is that it be short, relevant, easy to read, but with pointers to the full policies.

Short and relevant go hand in hand. Enlist a representative of your employee relations group to review the entire policy manual for policies—or even sections of policies—that matter to the average user. The Policy Organization section touched on some of them: acceptable use, information labeling and handling, e-mail, user access/passwords, virus prevention, and physical access. Still, there are other policies that may *seem* to be outside the realm of the average user's daily jobs, but have some relevance.

For example, employees who have laptops are likely to use them at home, for either work or personal reasons. An employee who has set up a home wireless network might think nothing of sliding a personally bought wireless card into his work computer and accessing his printer or Internet connection over the air. But if your organization has a policy prohibiting the use of wireless devices—because of the obvious security risks they pose—then that employee needs to know he cannot use his wireless home network. In short, a "wireless devices" policy may seem to be technical, but it can have implications for the average user.

The effort required to make the "lite" policies easy to read depends on how "techie" the original policies are. If the policies were written in a casual style, then an extensive rewrite may not be necessary. However, if your policy has language like this:

> The Corporation's information processing systems are authorized strictly for the purpose of accomplishing the Corporation's business. The use of the Corporation's information processing and communications systems for personal purposes is permitted provided that all of the following conditions are met.

Then you may want it simply to read:

> Your company PC, as well as the company's entire computing environment, is a tool to help you do your job. However, a certain amount of incidental personal use is acceptable, provided that it does not interfere with your ability to perform your job.

To enable users to gain a better understanding of their responsibilities, each section of the abridged policies should include a pointer, such as "For more details regarding acceptable use, please see policy X."

Something else the lite policy manual should do is explain. Your end users are adults, who are more likely to comply with a directive if they know *why* it is required. Therefore, telling users that they need to change their password every sixty days most likely will do little more than frustrate them. Explaining that if the password file was to be comprised, an attacker with typical resources could crack the average password within seventy days goes a long way toward putting the sixty-day expiration in context.

Finally, consider how to distribute the lite policies. At minimum, they should be posted to the company intranet in the same location as the full policies. If your policies are accessed from an "inside page," then maintaining a link on the "front page" of the company web site serves as a constant reminder of their (and, by extension, the full policies') existence.

Although it can be costly, depending on the size and geographical coverage of your organization, putting a copy in every user's hands ensures that users *see* them. In addition to taking away the "I didn't know . . ." defense, hard copies provide a convenient, easy-to-access reference source. Distribute them once to all employees, and then make them part of a new hire (including acquisitions) package.

CONCLUSION

Sports need rules, societies need laws, and organizations need policies. Although mundane (like rules and laws), policies provide an organization's members with an understanding of what is expected of them. Developing, maintaining, advertising, and enforcing a set of sound security policies help an organization protect its people and assets from harm, loss, alteration, abuse, and misuse, and allow the organization to continue to meet its stated business goals and objectives.

See also Information Security; Security Documentation; and Security Models.

NOTE

1. "RFC 2196, The Site Security Handbook," online at http://library.n0i.net/rfc/html/rfc2196.html (accessed 3 July 2006).

INTERNET AND E-MAIL USE POLICIES

W. Timothy Coombs

The Internet and e-mail have become integral parts of people's work lives. In the Unites States, over 40 percent of all workers use the Internet or e-mail on the job. That number continues to increase each year. We live in a wired work environment. There are positives and negatives to the Internet entering the workplace. The Internet increases efficacy by making information and people easier to access. Management surveys regularly show that the Internet has increased worker productivity. The Internet can also be a source of wasted time and lawsuits. These are two separate but important concerns that organizations attempt to address through Internet and e-mail use policies.

INTERNET AS WASTED TIME

It seems each new advancement in communication technology, such as the BlackBerry, is used to connect people to work. However, those connections also blur the line between work and nonwork. People use technology to work when they are at home so it seems only natural to use that same technology at work for some nonwork activities. People may use their work time to check the weather, stock prices, sports scores; to e-mail friends or family; or to pay bills. A number of experts argue that some personal time online is a good thing. Employees can take short breaks and manage their personal lives. The breaks can allow employees to feel refreshed during the day, much like a nap. By taking care of personal concerns, an employee can then better focus on the job. Employees may also have more time for work as the Internet allows them to more quickly complete personal tasks that could compete with work time.

Recently a New York judge ruled an employee could not be terminated for using the Internet for personal reasons.[1] The rationale was that the Internet is like reading the newspaper. It has both work and nonwork applications, so the employee should only be reprimanded.

But there is a concern about wasted time at work. Employees using the Internet, including e-mail, for personal use is known as cyberslacking. One study found that 90 percent of employees reported using the Internet for personal use while at work. Cyberslacking accounted for about one third of an employee's time online. Common cyberslacking activities include e-mailing friends and family, checking sports scores, booking personal vacations, bidding at auction sites, and shopping. Another study estimates that about $178 billion is lost annually in the United States to wasted personal Internet activity.[2] This lost revenue is a result of time spent on non-work-related web sites and sending non-work-related e-mails. The estimate is high and the company that conducted the study does sell software for monitoring employee Internet and e-mail activity, but there is no doubt that employees wasting time on the Internet is a cost. However, employees found ways to waste time at work long before the invention of computers and the Internet. In many ways, it is unrealistic and counterproductive to expect employees to work 100 percent of the time. A well-documented social aspect of work has been proven to increase task effectiveness. The problem is when the social aspect of work becomes unproductive or harmful. When the U.S. Congress released the Starr Report in 1999, some 13.5 million workers logged on to the government site to view the report during working hours.[3] Cyberslacking is a concern when it reduces worker productivity. Companies use Internet and e-mail polices, a point that will be addressed shortly, to prevent abuses that waste too much time.

HARM: ACTIONABLE ACTIVITIES

A bigger concern than cyberslacking is when employee use of the Internet or e-mail results in actionable activities—behaviors that create legal liabilities. This makes cyberslacking a security concern. Common actionable activities related to the Internet include sexual harassment, discrimination, defamation, and copyright infringement. Visiting pornographic web sites or sending sexually explicit text or pictures in an e-mail places an organization at risk for a sexual harassment lawsuit. The same holds true if people visit hate sites containing racist materials or send e-mails with text or graphics that are racially harassing. Employees can sue their employers for sexual or racial harassment and win. Chevron was sued and ordered to pay female employees $2.2 million to settle a sexual harassment lawsuit based on an offensive e-mail circulated by male employees.[4]

Defamation is a false statement that hurts someone's character or good name. Spoken defamation is known as slander whereas written defamation is known as libel. An employer can be held responsible if an employee commits libel in an e-mail as part of his or her job. Although there is some limitation to employer responsibility in libel cases, a risk still exists. The last actionable activity is copyright infringement. Copyrights are granted to protect intellectual property rights. Documents and works of art, for example, have automatic copyright protection. If an employee uses copyright protected works on the Internet without permission, including circulation in an e-mail, the employer can face liability for that action. Concerns also exist about downloading bootlegged music and movies. Managers should review the Intentional Inducement of Copyright Infringement Act of 2004, the Online Copyright Infringement Liability Limitation Act (OCILLA), the Computer Fraud and Abuse Act, and the enactment of the Economic Espionage Act of 1996 to get up to speed on these concerns.

HARM: DAMAGE RESOURCES AND INFORMATION

Employees can harm the computer system or information resources of an organization by misusing the Internet. Employees can degrade or slow down a network when they download music or movies legally. All the other employees suffer as the performance of the network is reduced. Forty employees at Xerox who were downloading videos clogged the network and other employees were unable to send or receive e-mail. Employees do not always follow safe computing practices and can introduce viruses into the company's system through downloaded files of e-mail attachments. Refer to the entry on Information Security for more details on viruses. Lockheed Martin's e-mail system once crashed for six hours because of a virus released by an employee.[5] That crash is estimated to have cost the company hundreds of thousands of dollars. Finally, employees have been known to give away trade secrets and proprietary information accidentally through e-mail correspondences. The entry on Corporate or Industrial Espionage discusses how corporate spies can dupe employees.

HARM: DAMAGE TO THE ORGANIZATION'S REPUTATION

Negative publicity can damage an organization's reputation. Reports of senior managers visiting pornographic web sites or of fines for pirated software on company computers can hurt an organization. The damage from inappropriate use of the Internet or e-mail can extend beyond the immediate financial damage when the story breaks and embarrasses the organization.

BOTTOM LINE

When employees use or misuse the Internet, an organization can be placed at a variety of risks. Some of the risks should be obvious, such as visiting hate or pornographic web sites, whereas others are subtler. Managers must take actions to reduce or to prevent the Internet-based risks. Security should be involved in these efforts. A combination of policies, training, and software solutions can be used to reduce organizational exposure to employee misuse of the Internet significantly.

IMPLICATIONS FOR INTERNET AND E-MAIL USE POLICIES

All companies that allow employees access to the Internet should have policies that govern the use of the Internet and e-mail while at work. The E-policy Elements box provides some suggestions for developing Internet and e-mail policies. Effective policies serve to protect the organization from legal liability. If an organization can document that an employee knew the policy, the individual employee is held accountable for the violation. The base of an e-policy is to identify what constitutes inappropriate activities. For e-mails, inappropriate includes using racist or sexist language or images, sending pornographic images, and distributing copyright protected materials. Unsuitable Internet sites would include hate sites and pornographic sites. Violation of these base policies should be grounds for termination. A 2005 study by the American Management Association found that 25 percent of organizations have fired workers for misuse of e-mail and 26 percent have fired employees for misuse of the Internet.[6]

E-policy Elements

Here is a list of the generic points to cover in an e-policy.

- Begin with a rationale for the Internet policy explaining why the organization needs it and why employees should follow it.
- If necessary, include a definition of technical terms used in the policy. Definitions ensure that employees understand what they are reading and agreeing to.
- Spell out "acceptable use," the core of the policy. Be very specific about what employees can do and cannot do on the Internet. Give examples of both acceptable and unacceptable actions. Unacceptable acts generally include infringing on others' copyrights, visiting sites that can be viewed as harassing, and using the Internet for noncompany commercial reasons. Be sure to include a list of the types of offensive sites to reinforce the point.
- State that you will monitor and enforce the policy. Remind employees that the organization retains the right to monitor all Internet activity. Detail how the Internet activity will be monitored and the penalties for violating the policy. Be sure to include any provisions that allow for personal Internet use.
- Include reminders about proper security measures while online and warn against downloading copyright protected materials.
- Provide a rationale for e-mail policies and define technical terms.
- List appropriate and inappropriate e-mail use. Give specific examples for both types of use. Common inappropriate e-mail use involves messages that include offensive, obscene, or racist comments and using copyright protected materials without permission.
- Remind employees that the organization retains the right to monitor all e-mail activity. Detail how the e-mail activity will be monitored and penalties for violating the policy. Be sure to include any provisions that allow for personal e-mail use.
- Include reminders about proper security measures when using e-mail.

Organizations can add a second layer to the policy that controls personal use of the Internet and e-mail. They can choose from a variety of personal use policies that include no personal use at any time, personal use during break times, a certain percent of e-mails or time on the Internet allowed for personal use, and no restrictions at all on personal use.

Enforcing Internet and E-mail Policies

No Internet or e-mail policy will be effective if management cannot detect and punish employees who violate the policy. Enforcing the Internet and e-mail policies is a multistepped process beginning with blocking software. Blocking software prevents many of the potentially actionable behaviors by employees. For the Internet, the software can block pornographic sites, hate sites, and other nonwork sites such as auctions and stock trading sites. Employees can still exploit holes in the blocking software or download programs designed to defeat the blocks. However, this shows purposeful action by the employee to violate the policies. Blocking software searches e-mails for inappropriate words and blocks those in violation. Again, only the most obvious violations can be caught. Over 65 percent of companies use some form of blocking software.[7]

In addition to blocking software, companies can monitor employee activities on the Internet and e-mail systems. This is a form of employee surveillance. Over 75 percent of companies use some form of employee surveillance for the Internet and e-mail.[8] These software programs scan employee activities for inappropriate behavior. The software can detect when employees visit web sites not designated as work-related or send e-mails that seem to be unrelated to work. The software can track where each employee has gone on the Internet and the amount of time spent at each site.

Surveillance polices can vary. The software can track all the employees all of the time, randomly, or only when a violation is suspected. Again, the distinction between harmful and personal use is important. A surveillance system should try to detect anytime the Internet or e-mail is used in a way that places the organization at risk, especially if an organization does not block pornographic and hate sites. The same holds true for actionable content in e-mails. The policy becomes more complicated for personal use. Software can be set to determine whether personal use is at nonbreak times or the computer is being used too often (beyond the amount allowed in the e-policy).

Communicating E-policies

All companies need to communicate their Internet and e-mail use policies to their employees. Some training may be needed but usually the policies are easy to understand and to follow. Just placing the e-policies in the employee handbook is not enough. A company can protect itself legally by having employees check a box each time they log on to their computers to acknowledge their knowledge and understanding of the e-policies. Companies must move beyond the legal to the human element of compliance. Make sure employees really know what the policies are, what constitutes a violation of the policies, and what the consequences are for violating the policies. Be sure to emphasize why e-policies are needed by providing examples of how misuses can harm a company. Moreover, disclose to employees how the company is monitoring compliance with the Internet and e-mail policies. The more employees understand the e-policies and monitoring, the less likely they are to violate them accidentally. This avoids having to terminate an employee for mistakes. Also consider building some flexibility into a system that includes which offenses should be zero tolerance and which should result in reprimands and training sessions.

Organization's Right to Monitor

Many news stories talk about Big Brother at work watching over employees. Some question the rights of organizations to read e-mails and monitor Internet use. The courts are firmly on the side of organizations. They reason that because the organization owns the computer system, management has a right to review what goes on in that system. This includes reading e-mails and tracking Internet use.

CONCLUSION

Management is not being responsible if it does not pay attention to how employees are using and perhaps abusing the Internet. The risk is too great not to have Internet and e-mail use policies. With policies comes the need to enforce them. Management must use some form of blocking software, monitoring software, or a combination of the two if its policies are to be taken seriously. If employees know management has no means of evaluating their Internet and e-mail use, they are less likely to comply with the policies. The Internet and e-mail are useful business tools. But these tools come with some risks, and e-policies coupled with blocking and monitoring software can reduce those risks and make the Internet and e-mail more of an asset than a liability.

See also Corporate or Industrial Espionage; Information Security; Reputation Management; and Social Engineering.

NOTES

1. "Judge Says It's OK for City Workers to Surf Internet," online at http://www.northcountrygazette.org/articles/042406WorkSurf.html accessed 15 Jan. 2007).

[2] "$178 Billion in Employee Productivity Lost in the U.S. Annually Due to Internet Misuse, Reports Websense, Inc.," 19 July 2005, online at http://www.websense.com/global/en/PressRoom/PressReleases/PressReleaseDetail/?Release=050719976 (accessed 10 Jan. 2007); and "Huge Losses Due to Internet Misuse," 19 July 2005, online at http://www.securecj.com/quarter2_2005/news6.php (accessed 11 Jan. 2007).

[3] "Money for Nothing," 3 Oct. 1998, online at http://news.bbc.co.uk/1/hi/events/clinton_under_fire/latest_news/185533.stm (accessed 15 Jan. 2007).

[4] Ann O'Neill (2005, Nov. 7). "E-mail Can Bounce Back to Hurt You," online at http://www.cnn.com/2005/LAW/11/03/email.legal/index.html (accessed 15 Jan. 2007).

[5] Daniel Braswell and W. Ken Harmon, "Assessing and Preventing Risks from E-mail System Use," 2003, online at http://www.treas.gov/usss/ntac/its_report_050516.pdf (accessed 12 Jan. 2007).

[6] American Management Association, "2005 Electronic Monitoring & Surveillance Survey: Many Companies Monitoring, Recording, Videotaping—and Firing Employees," 18 May 2005, online as http://www.amanet.org/press/amanews/ems05.htm (accessed 3 June 2005).

[7] American Management Association, p. 3.

[8] American Management Association, p. 3.

PORTABLE DEVICE SECURITY

W. Timothy Coombs

Current workplace trends include the use of cell phones, laptop computers, and personal digital assistants (PDA). These portable devices often have a wireless connection to the Internet. Although normal electronic security concerns still apply, portable devices raise certain unique security concerns as well.

PHYSICAL SECURITY

Physical security is a critical concern for portable devices because they are easy to steal. Thefts of laptops, PDAs, and cell phones are commonplace. The information stored on these devices can place organizations at risk. Some companies have had information compromised because employees left sensitive information on cell phones they had traded in. Always keep your portable devices in sight; never leave them unattended, even for short periods of time. Also, do not draw attention to your portable devices. Avoid using them in public areas. Consider using a carrying case that does not look like a laptop case. For laptops, make sure the system is password protected. Consider an alarm or lock for your laptop. Locks can be used to secure a laptop to furniture when you travel. Always back up your files just in case the device is stolen or damaged.[1]

INFORMATION SECURITY

For data security, think about using encrypted files. That way thieves would have a difficult time viewing files they were able to steal. Another option is to store files separately from the device. People can store the sensitive files on a CD, a DVD, or a removable flash drive. The large storage capability and small size make flash drives an excellent option. Carry the stored information in a different location from the device. A thief may get your portable device but not the vital information that could hurt the company.

Portable devices are like desktops. Keep them current with antivirus software and firewall protection. As with computers, attackers can gain access and take control of PDAs and cell phones. Although these devices do not carry as much information as computers, sensitive information can be compromised and your portable devices used for malicious ends. When you are not using remote connectivity, such as Bluetooth, disable the feature to prevent attackers from using the remote connectivity against you. Bluetooth is a specific type of technology used in wireless connections. Although many Bluetooth devices have security measures, attackers can "discover" your Bluetooth device and attempt to access it. Disable Bluetooth when not in use. And when using Bluetooth, employ the hidden mode so other users cannot find your device. In the hidden mode, devices are paired so that only they can find one another in hidden mode. You can execute a pairing in a secure area.[2]

WIRELESS CONCERNS

Many people now use wireless connection (WiFi) for business transactions. When employees utilize public wireless access points or hot spots, there is a danger that someone can intercept their connection. Attackers can exploit the network and/or gain access to sensitive information. For a wireless network, change default passwords regularly, restrict access to authorized users only, and consider encrypting data on the network.[3]

CONCLUSION

Portable devices and wireless connections make it easier for people to work when they are away from the office. However, employees need to be aware of the security risks they face and the actions they can take to become more secure.

See also Information Security; Physical Security; and Travel Overseas.

NOTES

1. Mindi McDowell, "Protecting Portable Devices: Physical Security," 2004, online at http://www.uscert.gov/cas/tips/ST04-017.html (accessed 5 Jan. 2007).

[2] Mindi McDowell and Matt Lytle, "Understanding Bluetooth Technology," 2005, online at http://www.us-cert.gov/cas/tips/ST05-015.html (accessed 5 Jan. 2007).

[3] Mindi McDowell and Matt Lytle, "Securing Wireless Networks," online at http://www.us-cert.gov/cas/tips/ST05-003.html (accessed 5 Jan. 2007).

INSIDER THREAT

W. Timothy Coombs

If you ask a security expert where the greatest threat to your organization's security is, the answer will be "Somewhere in your organization right now." Insiders are the most serious threat to information security. Employees, contract workers, or former employees are the most common insiders. Insiders know the system, have fairly easy access to it, and regularly use this advantage to wreak havoc on organizations.

NATURE OF INSIDER THREATS

The U.S. Secret Service and Computer Emergency Readiness Team (CERT) provide a detailed analysis of insider threats in the United States. Most inside attacks were executed by former employees (59 percent) or contract workers with the organization (41 percent). The majority of the former employees had had technical jobs at the organization including systems administrators, programmers, engineers, and IT specialists. Insiders were motivated by negative work-related events, work-related grievances, and revenge. Negative work-related events include firings, demotions, and disputes with other employees. The most common motive was revenge at 84 percent.[1]

CHARACTERISTICS OF ATTACKS

Insider attacks are rarely made without warning. Most attacks (80 percent) were preceded by inappropriate behavior such as arguing with coworkers, poor job performance, missing work, and being late for work. Many of the insiders (31 percent) had a history of disciplinary actions at the organization. Thirty-seven percent of the cases involved noticeable planning activity by the insider, while in 31 percent of the cases others had information about the impending attack including coworkers. A majority of insiders (58 percent) say they are upset and plan to harm the organization.[2]

Insiders attack by exploiting systematic vulnerabilities in applications, processes, or procedures. Remote access is the main route for attacks, which occur during nonwork hours. Insiders operate through compromised computer accounts, shared accounts, or unauthorized backdoor accounts they have created.

INSIDER ATTACKS AND THE ORGANIZATION

Most insider attacks were detected after an irregularity was noticed in the information system or the system became unavailable. Nonsecurity personnel primarily detected the events. Insiders do try to cover their tracks, and the system log has been the most common means for identifying the insider.

Insider attacks result in lost sales, stock price drops, governmental fines, lawsuits, lost consumer confidence, and damaged reputations. The attacks center on the organization's data, systems, and computers. Insiders sometimes target specific individuals rather than the entire organization. Organizations can suffer disrupted communication, lost sales, blocked customer contact, and damaged data.

LESSONS FROM PREVIOUS ATTACKS

Management needs to address negative work-related events and have a functional grievance system. Employees must feel they are being treated in a just manner. The entry Workplace Aggression provides additional details about the need to promote justice in the workplace. There are warning signs for attacks, and organizations should work hard to recognize them. Formal policies should be created for reporting potential attacks and communicated to all employees. Given that most insider attackers are former employees, organizations need strong policies for disabling access once an employee resigns or is terminated. Moreover, conduct background checks to be sure the organization is hiring the right people. (Refer to the entry Employee Background Screening and Drug Testing for more information.)

Be smart about employee access. Restrict right of entry to information using the "least privilege" principle. Each employee should have only the minimum access required to complete his or her job. Monitor employees who show warning signs such as arguments or missed work. Be sure to restrict remote access; it is the preferred route for insider attacks. Limit access to remote accounts and restrict the scope of remote access.

CONCLUSION

Not long ago, eight employees from four different banks sold more than 670,000 customer account records to identity thieves. The affected banks included Bank of America and Wachovia. Insiders can steal data, corrupt data, damage systems, or engage in a number of other activities that will harm an organization. Insider threats must be taken seriously; organizations should have in place plans, procedures, and policies designed to protect their information resources.

See also Contributors to Workplace Aggression; Employee Background Screening and Drug Testing; Information Security; Integrating Physical and Information Security; and Workplace Aggression.

NOTES

1. Michelle Keeney, Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall, and Stephanie Rogers, "Insider Threat Study: A Computer System Sabotage in Critical Infrastructure Sectors," 2005, online at http://www.treas.gov/usss/ntac/its_report_050516.pdf (accessed 12 Jan. 2007)

2. "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," May 2005, online at http://www.cert.org/insider_threat/ (accessed 2 Feb 2007).

SUSPICIOUS CYBER ACTIVITIES

W. Timothy Coombs

Certain warning signs indicate that your cyber security could be at risk. These risks include system failure or disruption, suspicious questioning, unauthorized access, unauthorized changes or additions, suspicious e-mails, and unauthorized use.

- System failure or disruption is when legitimate users have trouble accessing a network or web site. An example would be a denial-of-service attack.
- Suspicious questioning includes attempts to gain information about your system and its security via phone, by e-mail, or in person. An example would be someone asking about the configuration or your network.
- Unauthorized access includes failed or unsuccessful attempts to access your system or data.
- Unauthorized changes or additions include changes to a system's hardware or software that are not approved by the IT department.
- Suspicious e-mails include unsolicited attachments and requests for sensitive company information.
- Unauthorized use refers to people using the system for processing or data storage who have not been given clearance to do so.

These suspicious activities could be signs of larger problems and should be reported to the United States Computer Emergency Response Team (US-CERT).[1]

See also Information Security; and US-CERT (United States Computer Emergency Readiness Team.

NOTE

1. US-CERT, “Report Suspicious Cyber Activity,” online at http://www.us-cert.gov/reading_room/poster_2.pdf (accessed 5 Jan. 2007).

SOCIAL ENGINEERING: EXPLOITING THE WEAKEST LINK

Michael Seese

Many popular movies glamorize the life of the con artist. *The Entertainer*, *Dirty Rotten Scoundrels*, and *Ocean's Eleven* are three titles that come to mind. Whereas the exploits of these charming rogues make for good, escapist entertainment, scam artists are an all-too-real threat to the information security professional. Whereas the fictional fiends usually pull off amazing exploits that reap spectacular returns, it is the more mundane crimes that should be of greater concern to those of us in the real world. For while the $100 million heist portrayed in *Ocean's Eleven* certainly would “break the bank” of an average corporation, a $1,000 theft is easier to accomplish and, more importantly, easier to conceal.

The number of ways to commit theft in the information age is countless. Some reports speak of a one-time criminal foray into a corporation's accounts payable system, whereby the intruder creates a nominal recurring bill—say, $19.95 per month—that won't raise many eyebrows. Done once, it's a small payoff, albeit one which can continue in perpetuity. If done to thousands of accounts, it becomes a large, steady stream of income. Stolen laptops or compromised databases that contain credit card numbers or Social Security numbers clearly are desirable targets. And, it is not unheard of for a criminal to steal sensitive information and then extort money from the data's owner in exchange for neither releasing it nor simply divulging that the theft occurred.

The attack strategies mentioned above can and do happen. However, like the fictional casino heist in *Ocean's Eleven*, they often are undertaken by large criminal organizations seeking a huge payoff. More common are the smaller schemes by lone individuals. In some cases, the attacker uses technical means to circumvent the corporation's controls. In others, however, the thief employs charm, guile, and wit to secure information—or perhaps even direct systems access—in order to achieve the goal. Individuals who use this tactic are referred to as social engineers.

A term commonly used in the information security field is the *low-hanging fruit*. If a criminal wants something specific to a given organization, that person will keep attacking until he or she either gets it or gets caught. Others, however, simply go after the low-hanging fruit . . . the easiest target. If the organization puts up the proper technical roadblocks, the criminal will move on. But as the technological information security solutions continue to improve, those seeking to gain unauthorized access to our systems will focus on the weakest link: our people.

Social engineers succeed because people are people. They want to help. They want to be left alone to do their jobs. They don't want to be yelled at. They trust. In some cases, they are greedy. But often, they simply don't realize the value of what, to them, seems to be a trivial piece of information. The social engineer takes advantage of our human characteristics to exploit us, tricking us into breaking normal security procedures.

SOCIAL ENGINEERING CLOSE TO HOME

A familiar form of social engineering is the various e-mail scams that bombard our electronic inboxes. One that, by now, probably every existing e-mail address has received is the Nigerian wealth scam. The e-mail begins something like, "Dear Friend, I need your help in retrieving my millions of dollars. Just send me your bank account number so I can deposit. . . ." Another common ploy is the Spanish lottery, which promises millions in prize money if the "winner" would only send back to the e-mail's sender the requisite taxes (which inexplicably can't simply be withdrawn from the winnings).

Included in e-mail scams are "phishing" attacks. Now as common as the simple scams described above, phishing attacks purport to originate from a financial institution and ask (though sometimes warn) users to update their personal account information by clicking on the attached link and providing what is required. These schemes do require a little more work on the part of the attacker, as the e-mail often carries the logos of the organization (which now can be considered a victim as well) and financial entities such as the FDIC or the Better Business Bureau; and the embedded link takes the recipient to a web page that usually is a detailed copy of the victim institution's web site. The success of the phishing attack has spawned a variety of "improvements," including the following:

- Spear phishing, which involves sending the fraudulent e-mail only to customers of the institution in question, in contrast to a standard phish e-mail, which is sent to as many e-mail addresses as the scammer can find.
- Vishing, which leverages voice-over IP (VoIP) technology to dial victims with a message that their credit card has had recent fraudulent activity. The victim is asked to type in his or her credit card information.
- Smishing, whereby a text message is sent to cell phone users, usually informing them that they have enrolled in a service of some sort and will be charged unless they visit a listed web site to unsubscribe. Visiting the site loads malware on the victim's computer.

The Anti-Phishing Working Group (http://www.antiphishing.org/) is "the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming, and e-mail spoofing of all types." The site features news, examples of recent phishing e-mails, and the victims' sites, along with statistics that often prove to be quite chilling. A sample includes the following:

- Number of unique phishing reports received in July 2006: 23,670
- Number of brands hijacked by phishing campaigns in July 2006: 154
- Average time online for site: 4.8 days
- Longest time online for site: 31 days[1]

Other crime statistics on telephone fraud, identity theft, and organized crime are equally unsettling. Telephone scams, such as tricking users into dialing a 10xxx or 1010xxx code—used to select an alternate long-distance carrier on a per-call basis—costs victims an estimated $4 billion per year.[2] The 2006 Identity Fraud Survey Report, released by Javelin Strategy and Research and the Better Business Bureau, found the following: while the number of U.S. adult victims of identity fraud decreased from 10.1 million in 2003 to 8.9 million in 2006, the mean fraud amount per fraud victim rose from $5,249 to $6,383 and the mean resolution time increased from 33 hours per victim to 40 hours per victim.[3] And Shadowcrew.com, which established a repository of stolen credit cards and identity documents, reportedly made $8 million over two years.[4] Further, a recent online article noted that San Diego computer security company Websense estimated that "during the first half of 2006 there was a 100 percent increase in sites designed to install forms of 'crimeware' that could log keystrokes or record information entered into online forms. Altogether, Websense counted 16,663 sites that carried code for stealing passwords, including banking passwords, during that period."[5]

The original, or at least most well known, social engineer is Kevin Mitnick. Between 1979 and 1995, he used his skills to gain physical and logical access to numerous corporate and government entities, including the computer systems of Fujitsu, Motorola, Nokia, and Sun Microsystems. He ultimately was caught and served five years in prison. As part of his probation, he was forbidden from using any communications technology other than a landline telephone, though a judge later overturned that restriction and granted him to access the Internet. His exploits are detailed in the book *The Art of Deception*, a must read for all information security practitioners. (If you don't want to buy the book to avoid paying a criminal for his deeds, get it from the library.) He now earns an honest living as a speaker and a security consultant. Though the authorities caught up with Mitnick, his spirit lives on in countless others, as evidenced by the traffic at http://www.socialengineering101.com, a site that offers social engineers possibly every tool they ever could need, including a chat board for sharing recent successes and failures.

PHYSICAL ATTACKS

Although there are many ways to classify social engineering attacks, one simple distinction is physical versus psychological. A physical attack, simply put, is sneaking in . . . though in some cases the social engineer may strut in.

A common ploy is to appear like someone who *should* be on the premises. A delivery person or a copier repair technician often is anonymous—and almost faceless. The simple truth is that most employees would not give such a person a second look. Being anonymous helps the social engineer attain his primary goal, which is access. Once in the building, he has many options. He could find an unsecured telecommunications closet and install telephone eavesdropping equipment, or perhaps a wireless access point. He could locate an unoccupied office, plug in his own laptop, and attempt to compromise the network from safely inside of the corporate firewall. He could look for a logged-in PC and access the network—or the PC's contents—through that avenue. He could install a keystroke logger. He could steal a user's credentials by "shoulder surfing," or simply watching as the employee logs in, and then exploit the network from home later. He could steal a laptop. Or, he simply could steal documents, either those showing corporate or customer information, or others that might seem innocuous, but that could prove valuable to him later. Even something as simple as a calendar can provide the social engineer with vacation schedules he can use to his advantage. It is not unheard of for a truly dedicated social engineer to take a job with a cleaning company so as to have unsupervised after-hours access to a facility.

A variation of the physical attack is to don a suit and walk in with an air of authority. This subterfuge, often used by someone trying to enter a facility that requires a card swipe to gain entrance, is accompanied by a plea to "piggyback," such as "I'm late for a meeting and I left my badge at my desk."

Another tactic is the "dumpster dive." As long as the attacker isn't afraid to get a little dirty, this criminal potentially could find a wealth of information that was discarded without being shredded. A financial institution could carelessly toss account information; any organization could throw away the personally identifying information of its employees. Even if the discarded documents don't contain any of the aforementioned "immediate payoff" items, a talented social engineer still could find treasure in another man's (literal) trash. For in addition to the physical attacks described above, the social engineer also can launch a psychological attack, whereby he uses his wits and any small crumbs of data he finds to craft a plausible reason for someone to give him what he needs.

PSYCHOLOGICAL ATTACKS

Mitnick tells the story of Stanley Mark Rifkin who, in 1978, stole $10 million from the now-defunct Security Pacific National Bank of Los Angles using his knowledge of wire transfer procedures and a little number he found written on a piece of paper.[6] Admittedly, Rifkin found the piece of paper because of his legitimate physical access as a consultant. Still, it just as easily could have been tossed with the trash and used by someone with sufficient knowledge of a bank's wire transfer process.

Psychological attacks play on the same human qualities that make e-mail scams work. The variations literally are endless. The attacker could call the help desk, claiming to be an executive locked out of his account and requesting immediate access in order to get some necessary files. If the help desk employee hedges, the "executive" demands to know the name of his or her supervisor and basically threatens some form of corporate sanctions.

The call could come from the executive's administrative assistant, who pleads that she needs to have her boss's password reset, because she fat-fingered it and must get back in right away to update some important files that he'll need for a meeting after lunch. Rather than take a headstrong approach, she tries to gain sympathy, claiming that she already has locked him out twice this week, and that he would not take too kindly to having to place a third request.

Or, the social engineer could pose as someone from the help desk, call the administrative assistant, and explain that he needs her boss's credentials in order to install the new secured screen saver remotely.

An interesting combination of the physical and psychological, from the Mitnick files, describes an after-hours foray into a helicopter assembly plant. The intruders were caught by a guard and taken to the security center. Having done his "homework," the intruder was able to assume the name of a legitimate employee and supply his supervisor's name as well. The guard called the manager—bear in mind, it was the middle of the night—explained why he was calling, and handed the phone over. The "employee" apologized for not checking first to see whether the visit was OK, chatted with his boss for a few minutes, said he would see her in the morning, hung up, bid the security staff good night, and made a hasty retreat. It was not until fifteen minutes later, when the manager was able to get through to the guard station and asked, "Who the hell was that who just talked to me?" that the guards realized they'd been had. Although this scenario was more of a "joyride" and resulted in no loss to the company, it is not hard to imagine the sabotage or thievery that *could* have taken place.

COMBATING SOCIAL ENGINEERS

"Traditional" attack methods have well-established countermeasures. To prevent physical intrusions, erect a perimeter fence, install exterior and interior surveillance cameras, and hire a security force. To stop network-based attacks, install the proper technological solutions, such as firewalls and intrusion prevention systems, and secure the computers themselves through OS patching and the installation of an up-to-date antivirus program. But thwarting social engineers is not a matter of procuring and installing something. In all cases, the basic countermeasures for social engineering attacks are sound policies and the education of your staff.

Although everyone in the organization must understand what social engineers are and how they operate, it is the end users who must be the focus of any training effort. End users often are the target. They are the largest corporate population, they work with the critical (and, therefore, desirable) information, and they just want to do their jobs. But, they also want to do the right thing. So intelligent, well-written directives and adequate, engaging training give them the necessary tools to do their part to safeguard the organization's information assets.

SOUND POLICIES

In large organizations, seeing unfamiliar faces is common. A social engineer realizes this and banks on the fact that to most people he or she will appear to be just another new employee. But if your policies require all employees and visitors to wear visible badges, someone without a badge will stand out. Further, all visitors should be asked to sign in so that your front-desk guards can issue them a temporary, expiring badge, which will prevent them from reentering the premises at a later date. Sound practice also requires all visitors to at least display—if not leave—some form of photo identification such as a driver's license. If a social engineer is prepared, he may come equipped with a fake ID. But if not, he or she has a choice: show one's real credentials or balk at the request, thereby raising (one would hope) the guard's suspicions. Further, all visitors should be greeted at the front by the employee they are scheduled to meet. Having such a policy in place does not allow the guard the leeway to circumvent the process and say, "I'm sure you know the way. Go on ahead." Nor will the guard have to apologize for making the visitor wait for his or her contact.

Because many physical attacks are enabled by a seemingly innocuous person walking through the building, set a policy such as "No outsider may wander the facility unaccompanied." Additionally, employees should offer to "help" an unescorted visitor. Is it inconvenient for an employee to have to walk a legitimate visitor—such as a vendor—to the restroom? Probably. But will it make someone who is in your facility illegally stick out? Definitely.

Mitnick cites a common tactic whereby a well-dressed person knocks on the facility's doors after hours and convinces a member of the cleaning staff to admit him or her. The solution to that deceit is having a policy that requires employees to provide a company ID badge for after-hours admittance, with no exceptions. Such a policy takes the pressure off the cleaning crew, who then can reply, "I'm sorry, sir, but you'll have to call security. It's out of my hands."

If employees know that they will not be penalized for taking that extra step—even though it may mean risking inconveniencing another—then situations such as the one described above are less likely to arise.

In short, any written policies that do not allow someone to bend the rules—”just this once”—will improve the organization’s security posture.

REAL-WORLD TRAINING

The aforementioned policies should be reinforced by periodic employee education. This training not only must demonstrate to employees how social engineers operate but also should emphasize how valuable the data they use truly are—no matter how insignificant these data may seem—and show them how to protect data.

To underscore the significance of an “insignificant” bit of information, Mitnick recounts an example in which a private investigator attempted to determine whether his client’s soon-to-be ex-husband had opened any new accounts in his own name in order to hide marital assets.[7] He first placed a call to a bank branch to confirm that it used a given credit reporting bureau and asked when the identifier it supplied the bureau is called a “merchant ID.” When the bank employee seemed hesitant to provide this information, Mitnick explained that he was writing a book and simply wanted to make sure he had the term correct. Satisfied with that explanation, the employee confirmed that it was the proper term. Because the investigator felt he had aroused her suspicions, he didn’t try to press her for the ID itself. Instead, he called another branch and, pretending to be from the credit bureau, said he was performing a merchant satisfaction survey. In the middle of about a dozen questions, he asked for the bank’s merchant ID. After securing that final piece, he made a third call to the credit bureau, used the merchant ID he had just obtained to pose as an employee of the bank, and inquired into the recent activity of his client’s husband. The lesson here is that social engineers often take advantage of the fact that people simply are not aware of the value of the information they possess—after all, what is the harm in sharing the term *merchant ID*—and are careless about protecting it.

Although your organization could utilize one of the traditional corporate training methods, such as computer-based training (CBT), a hands-on, role-playing approach probably would work best. First, it’s more entertaining and therefore more likely to engage your employees. Second, it’s one thing to explain what a social engineering attack is. Having a social engineering attack unfold before their eyes and letting employees see what two innocent phone calls can produce, is an entirely different matter. And finally, whereas a CBT (even one that has been updated) might seem to be a chore after the third or fourth run-through, an interactive session portraying the latest attack methods always should seem fresh.

The idea is to train your people to recognize signs of social engineering attacks, such as refusal to give *back* adequate information or an explanation, expressing a sense of urgency, providing names with no context, intimidating, and the outright requesting of sensitive information.

Because many social engineers use the phone as their weapon of choice, a primer on telephone security best practices also would be in order. Encourage employees to write down the name and number of everyone who calls, and to emphasize that they are doing so. Asking the callers to spell their names and repeat their phone numbers tells them that the person on the other end of the phone is paying attention, rather than handling this latest “fire drill” and getting back to the task at hand. Many modern PBX systems show the phone number of the caller, which should be compared with the number provided. Still, your employees cannot rely on the display, because phone numbers can be spoofed—though spoofing an internal number is more difficult. And, logging the time of the call can help piece together information after the fact if an investigation of some sort is required.

Something that favors social engineers is the fact that their reconnaissance missions often are conducted remotely. If they are discovered, they can move on. Again, consider the contrast with an attack on a network: if the firewall team sees unusual activity coming from a certain IP address or targeting a segment of its network, team members can put up specific barriers in response. On the other hand, if a social engineer’s questions arouse the suspicions of the persons on the other end of the line, the social engineer can simply hang up the phone and dial another number. Even if the organization is small enough to allow the would-be victim to spread the word, chances are the attacker will strike again before word can get around.

Therefore, your organization should foster and project an aura of preparedness. Social engineers’ success is attributable, in part, to the ability to remain cool, quick, and clearheaded under pressure. Therefore, anything that instills a hint of indecision should hamper their efforts. A proper response to inquiries ought to cause social engineers who are contemplating breaking in to wonder whether their story, or even their mere presence, will single them out. As mentioned earlier, if they want something unique to a specific organization, they will keep trying. But if they are seeking an easy target, they likely will move on.

CONCLUSION

An attack on a network follows a sort of cookbook: scan the perimeter for services that are “listening,” try to determine the identity of that service, determine whether it has any known vulnerabilities, and then exploit one. Social engineering, in contrast, is a method of attack that can take on a seemingly limitless number of variations. In short, the social engineer seeks out clever ways of getting questions answered and then using that information to gain access to sensitive information or physical spaces. The permutations are endless: these criminals could seek information in an effort to gain physical access, they could seek information in order to gain logical access, or they could use physical access as a means to the information immediately or logical access later. Because the attack can take on so many different forms, there is no simple countermeasure. Instead, organizations must establish, publicize, and enforce strict policies regarding physical and logical access and information sharing. Then, the organization's employees must be provided with engaging, realistic training in order to prepare them for the possibility that they will someday have to fend off a social engineer. Although humans can't be set with an absolute rule—like "deny all" in a firewall's rule set—they can be provided with a variety of scenarios, and then use intelligence and experience to apply their best judgment to the situation at hand.

See also Corporate or Industrial Espionage; Information Security; and Insider Threat.

NOTES

1. "Phishing Activity Trends Report July, 2006," online at http://www.antiphishing.org/reports/apwg_report_july_2006.pdf (accessed 3 Dec. 2006).

2. "Fraud Education: Scams, Schemes, and Some Simple Safeguards," online at http://www.consumer.att.com/global/english/consumer_information/fraud.html (accessed 17 Dec. 2006).

3. "Javelin/Better Business Bureau Survey—January 2006," online at http://www.privacyrights.org/ar/idtheftsurveys.htm#BBB06 (accessed 17 Dec. 2006).

4. Lippis Consulting, "Building Trusted Networks: Gaining Control Of IT Security," January 2006, online at http://www.hp.com/rnd/pdfs/lippis_whitepaper_trusted_networks.pdf (accessed 17 Dec. 2006).

5. Elisa Ackerman, "Hackers' Infections Slither onto Web Sites," 3 Jan. 2007, *Mercury News,* online at http://www.siliconvalley.com/mld/siliconvalley/news/local/16374909.htm (accessed 4 Jan. 2007).

6. Kevin Mitnick and William Simon, 2002, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis, IN: Wiley Publishing, 2002), pp. 16–21.

7. Mitnick and Simon, *The Art of Deception*, pp. 4–6.

DATA BACKUP

W. Timothy Coombs

You have probably read and heard many times that data are the lifeblood of your organizations. Because data are an irreplaceable strategic asset, loss or destruction of data can have horrific financial consequences for an organization. Among the critical data are customer records, employee records, and outstanding accounts. Compromised or lost data can mean a damaged reputation, reduced investor confidence, regulatory violations, lost customers, lost cash flow, and competitors acquiring your data. A number of entries in this collection have addressed ways to secure an organization's data.

Anyone who has used a computer knows the risks of electronic data. Power outages or viruses can damage or erase data. Organizations can also experience disruptions such as planned outages, system maintenance upgrades, or hardware and systems failures. At times, larger-scale disruptions can occur as a result of fires or major weather disasters. Organizations do need a reliable system for backing up their data. A common term used to refer to a number of different backup concepts is *e-vaulting*.

Data backup is part of data archiving. You store data in order to recall and use it at a later data. You back up data so that if data are lost, corrupted, or stolen, they can be replaced. Data recovery is initiated and the original data replaced by backup data. This is a familiar process to anyone involved in disaster management. A number of options for backing up exist, including in-house options, remote options, tapes, disks, data compression, and encryption. This entry discusses the various backup approaches.

STORAGE OPTIONS

Data can be stored in different formats. Two common options are tapes and hard drives. Tapes were among the first backup storage formats but have a number of problems. First, they take up a lot of physical space, are difficult to organize, and result in a slow recovery time. Second, tapes have a history of failure. Surveys regularly find that around 50 percent of tapes have flaws or are missing data when used to restore data. Tapes are also easy to steal or to misplace.

More organizations are moving to hard drive storage because it requires less storage space, data are easier to organize, and recovery time is faster. Data files can be compressed, further reducing the storage space. Of course, data can still be stolen from hard drives and the electronic transfer of information. Encryption can be used to protect the data when they are transited and stored. The use of encryption is discussed further in the next section.

Another factor to consider is when and how the data are backed up. Older systems rely on manual backup. A user executes a command to back up the data. This could be done at the end of the day, every hour, or at some other time interval. A software program executes the automatic backup, rather than a person who can forget to back up the data. The program decides when to back up the data. Many programs now permit real-time backup of data. *Data mirroring* is a term used to refer to the real-time backup of data.

IN-HOUSE AND THIRD-PARTY OPTIONS

Some organizations prefer to back up data in-house. In-house backup guards against data being lost or stolen while being transferred to or stored by a third party. The threat is to both tapes and electronically transferred data. For in-house backups to work, the organization has to have the necessary IT infrastructure and support. It is best that the backup does not reside at the same physical site as the original data. If the original data are destroyed by weather disasters or fire, the odds are the backup will suffer a similar fate if it is at the same location. There are the security concerns when transferring data and thus a need for encryption.

Many organizations turn to third parties for their data storage needs. These data storage vendors provide a variety of options for backing up, recovering, and archiving data. For instance, some backup choices include recovering a specific file, all files from a specific machine, or all of the organization's data. The data storage vendors enable quick and easy access and can help ensure regulatory compliance for data storage. If you use a vendor, test its recovery time with annual or semiannual recovery drills. The third parties will be off-site so you have the added security of separating the original and backup data.

Security of the data, electronic and physical, is a concern with third parties. Data should be encrypted for transmission and storage. Only you should have the encryption key. The third party must not have a key or any backdoor means of accessing your data. Check the physical security of the data storage vendor as well. How secure are the servers, and what measures are in place to protect the servers from unauthorized access? Most vendors have strong physical and IT security because it is a selling point for clients. Management needs to consider the cost relative to the benefits of each option when choosing between in-house and third-party data backup.[1]

CONCLUSION

Data backup, or e-vaulting, tries to keep data safe by having a backup to replace lost, corrupted, or stolen data. Automated backup is best because it reduces the likelihood of human error. Real time or near real time is preferable because delays in backup can result in lost data. Hard drives appear to be more reliable than tape backups, and backup data should be stored in a different geographic location from the original to prevent the same event from destroying the original and backup versions of the data.

See also Information Security; and Integrating Physical and Information Security.

NOTE

[1] "The Many Faces of E-vaulting Can Confuse IT Efforts," 1 Nov. 2006, online at http://www.computerweekly.com/Articles/2006/11/01/219586/the-many-faces-of-e-vaulting-can-confuse-it-efforts.htm (accessed 30 March 2007).

US-CERT (UNITED STATES COMPUTER EMERGENCY READINESS TEAM)

W. Timothy Coombs

The U.S. government recognizes the danger of cyber attacks on national security and business. In 2003, US-CERT was created to help protect the country's infrastructure. This unit coordinates response to and defense from cyber attacks. It can be found on the Web at http://www.us-cert.gov/. The US-CERT web site provides information on how to improve cyber security along with warnings about newly identified threats and the opportunity to report vulnerabilities. Advice on cyber security can be found in the publication section, which also contains regular publications about various updates regarding vulnerabilities and threats.

There are three regular types of publications: Technical Cyber Security Alerts, Cyber Security Alerts, and Cyber Security Bulletins. Technical Cyber Security Alerts are designed for systems administrators and technical users. These publications provide information on security issues, vulnerabilities, and exploits. Cyber Security Alerts are for home and corporate users and cover security issues and vulnerabilities. Cyber Security Bulletins are for systems administrators and contain summaries of published information about new vulnerabilities. Users can sign up to have both the Technical Cyber Security Alerts and the Cyber Security Alerts e-mailed directly to them. These two alerts contain roughly the same information. In 2006, US-CERT issued thirty-nine Technical Cyber Security Alerts, thirty-seven Cyber Security Alerts, and fifty-one Cyber Security Bulletins. See the Sample US-Cert Cyber Security Alert box.

Sample US-Cert Cyber Security Alert

Mozilla Addresses Multiple Vulnerabilities

Original release date: December 20, 2006
Last revised: --
Source: US-CERT/UL

Systems Affected

- Mozilla Firefox
- Mozilla Thunderbird
- Mozilla SeaMonkey
- Netscape Browser

(continued)

Other products based on Mozilla components may also be affected.

Overview

Mozilla Firefox, Thunderbird, and derived products contain several vulnerabilities. By taking advantage of one or more of these vulnerabilities, an attacker may be able to take control of your computer.

Solution

Upgrade to the Latest Versions of Firefox, Thunderbird, and SeaMonkey/3

Mozilla has released Firefox 1.5.0.9, Firefox 2.0.0.1, Thunderbird 1.5.0.9, and SeaMonkey 1.0.7 to correct these problems. Mozilla Firefox, Thunderbird, and SeaMonkey automatically check for updates by default.

Security updates for Firefox 1.5 are scheduled to end in April 2007. According to Mozilla:

> *Firefox 1.5.0.x will be maintained with security and stability updates until April 24, 2007. All users are strongly encouraged to upgrade to Firefox 2.*

Disable JavaScript and Java/3

These vulnerabilities can be mitigated by disabling JavaScript and Java. For more information about configuring Firefox, please see the “Securing Your Web Browser” document. Netscape users should see the “Site Controls” document for details.

Thunderbird disables JavaScript and Java by default.

Description

Mozilla products, including the Firefox web browser and Thunderbird email application, contain a number of vulnerabilities. These vulnerabilities may allow an attacker to access your computer, run programs that could cause your computer to crash, or gain control of your computer. An attacker could exploit these vulnerabilities by convincing you to visit a web site or read an HTML formatted email message.

For more technical information, please see US-CERT Technical Alert TA06-354A.

(continued)

References

- US-CERT Technical Alert TA06-354A—http://www.us-cert.gov/cas/techalerts/TA06-354A.html
- US-CERT Vulnerability Notes—http://www.kb.cert.org/vuls/byid?searchview&query=mozilla_20061219
- Securing Your Web Browser—http://www.us-cert.gov/reading_room/securing_browser/browser_security. html#Mozilla_Firefox
- Mozilla Foundation Security Advisories—http://www.mozilla.org/security/announce/
- Firefox—Rediscover the Web—http://www.mozilla.com/firefox/
- Thunderbird—Reclaim Your Inbox—http://www.mozilla.com/thunderbird/
- The SeaMonkey Project—http://www.mozilla.org/projects/seamonkey/
- Mozilla Hall of Fame—http://www.mozilla.org/university/HOF.html
- Site Controls—http://browser.netscape.com/ns8/help/options-site.jsp[1]

The US-CERT program works closely with CERT, a center for Internet security that is part of the Software Engineering Institute operated by Carnegie Mellon University. CERT members write most of the US-CERT publications. CERT is dedicated to studying Internet security vulnerabilities and providing ways to improve security. Why the concern about vulnerabilities? In 2000, a total of 1,090 vulnerabilities were reported. That number has risen to 5,990 in 2005 and 8,064 in 2006. US-CERT and CERT are important resources for those wanting to stay current on the latest Internet vulnerabilities, one part of the larger cyber security picture. The CERT Charter states:

> CERT is chartered to work with the Internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents. In particular, our mission is to
>
> - Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
> - Facilitate communication among experts working to solve security problems.
> - Serve as a central point for identifying and correcting vulnerabilities in computer systems.
> - Maintain close ties with research activities and conduct research to improve the security of existing systems.
> - Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.[2]

See also Information Security; and Suspicious Cyber Activities.

NOTES

1. US-CERT, "Mozilla Addresses Multiple Vulnerabilities," online at http://www.uscert.gov/cas/alerts/SA06-354A.html (accessed 28 Jan. 2007).

2. CERT, "Appendix A: The CERT Charter," 26 Feb. 2007, online at http://www.cert.org/meet_cert/meetcertcc.html (accessed 14 April 2007).

TERRORISM AS A BUSINESS SECURITY AND SAFETY CONCERN

Terrorism remains a concern for both domestic and international organizations. The tragic events of 9/11 raised awareness of an often overlooked area of business security and safety concern. However, terrorism had been a concern well before 2001. This section reviews some of the types of terrorism and considers the unique security concerns of chemical facilities and organizations involved in the food industry.

TERRORISM

W. Timothy Coombs

Terrorism is to some degree a political term. It becomes political when people debate the motives of groups engaging in violent acts. This entry focuses on a more descriptive approach to terrorism. The purpose is to identify why terrorism is a business security issue and to explore the nature of that issue.

In the United States, an accepted definition of terrorism is "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[1] In general, terrorism employs violent actions to create anxiety in order to achieve some political or social goal. Terrorism is goal directed and pursues those goals with no regard for life or social norms.

DYNAMICS OF TERRORISM

Terrorism is often indirect as the targets are not the ones who will make the decisions. The terrorist act is a form of communication. The terrorists are sending a "message" to the people who can create change. That message has two parts: (1) to create fear among people and (2) to convey their demands or ideas to other people. Terrorism benefits from news coverage of an event, something also known as publicity. Publicity helps both to spread fear and to state the terrorist's goals. The news media are drawn to conflict stories and unusual events. The violent terrorist acts embody both characteristics of a good news story. Terrorist acts are designed to be visible. Businesses and their employees can find themselves victims of this violence.

TYPES OF TERRORISM

In the United States, terrorism is divided into two categories: domestic and international. Domestic terrorism occurs inside the United States. International terrorism occurs outside of the United States or crosses national boundaries depending on where the terrorists operate, where they seek asylum, the means they use to conduct an attack, or the people they are trying to intimidate or coerce. Businesses or their employees can be victims of either domestic or international terrorism.

As terrorist expert James A. Johnson notes, too often businesses have thought of terrorism as something that happens "over there." However, domestic terrorism has long been a reality in the United States, and international terrorism has shown that it can extend its reach to the United States.[2] Special-interest domestic terror organizations have been on the rise since the 1980s. These groups try to influence specific issues rather than promote major political change. They use violence to try to inform the public about an issue and attempt to change public opinion on that issue. Ecoterrorists are an example of special-interest domestic terrorism. (See the Ecoterrorism entry for more information on this subject, including the number and types of attacks.)

GROWING CONCERN ABOUT TERRORISM

The attacks of 9/11 and the first World Trade Center attack illustrate that international terrorism can touch businesses in the United States as well. It is no surprise that business security has risen as a priority and budget item since the attacks of 9/11. The U.S. Department of Homeland Security (DHS), through its Ready.gov web site, emphasizes to all businesses that terrorism is a concern. In "Preparing Makes Business Sense," DHS uses the 1993 World Trade Center attack, the 1995 Oklahoma City bombing, and the September 11, 2001, attacks to highlight the importance of being prepared.

It should be noted that although terrorism is a recent priority, it has long been a threat to U.S. companies. The Federal Emergency Management Agency (FEMA) recognizes that a human-caused hazard such as terrorism can occur at any facility.

The rising concern of terrorism is directly linked to business security. In 2002, surveys began documenting the new emphasis on security; health, safety, and environmental coordinators were rating security as their number-one budget item and priority. In a 2003 survey of business executives by the Council on Competitiveness, 88 percent of executives rated security the number-one priority, 65 percent had adopted new security procedures in the past year compared to 53 percent the previous year.[3] Terrorism has risen as a threat/hazard for organizations. Physical security, often in the form of the ability to control entry into and egress from a building, securing perimeters, and monitoring people in buildings, was being strengthened to prevent terror attacks. The growing concern over agroterrorism in the United States is another example of how international terrorism is a rising concern. (See the Agroterrorism and related entries for details on this particular type of terrorism.) Information security requires attention as well because terrorists can employ cyber attacks.

Outside of the United States, businesses have also long been established terror targets. From 2000 to 2006, U.S. government statistics identified business facilities as the target in 673 terrorist incidents, excluding Iraq and Afghanistan. The 27 attacks in which employees were victims of terrorism resulted in 205 injuries, 6 hostages, and 41 fatalities. In terms of direct monetary damage, 28 incidents caused over $500,000 in damage. Researchers estimate that the indirect costs are even greater. Indirect costs include a negative impact on the stock prices of businesses targeted by a terror attack. Some of the U.S. firms affected by terrorist attacks include Coca-Cola, McDonald's, and American Airlines. The names of these companies are closely tied to the United States, making them very attractive targets.[4]

Terror attacks against businesses have occurred in a number of locations around the world including India, France, Spain, Colombia, Nepal, Turkey, Thailand, Pakistan, Saudi Arabia, Bulgaria, Algeria, the Philippines, Ghana, Sri Lanka, and the Sudan. Many of these locations have a history of terrorism. Others we might not think of as terrorist risks. The Travel Overseas entry discusses resources available for assessing the terrorist threat in an area and warnings of recent threats or activities. Refer to this entry for more information on the topic of employee safety overseas. Companies need to think beyond their U.S. facilities to the security of overseas facilities and the safety of their personnel traveling overseas.

CONCLUSION

In recent years, organizations have improved physical security to prevent terrorist attacks. The post–9/11 attacks response is neither an overreaction nor misguided. Terrorism is a real threat in the United States and abroad. No area is truly immune from terrorism, and attacks are becoming more unpredictable. Risks do warrant countermeasures. Moreover, improving security addresses a number of other vulnerabilities, such as workplace violence, and readies employees to be better prepared for any emergency situation. Terrorism, both domestic and international, is a legitimate risk that should influence business security measures. The impact will be felt on security at domestic facilities, overseas facilities, and guidance for employees traveling abroad.

See also Agroterrorism; Customs-Trade Partnership Against Terrorism; Ecoterrorism; and Travel Overseas.

NOTES

1. Federal Bureau of Investigation, "Terrorism 200/2001," 2002, online at http://www.fbi.gov/publications/terror/terror2000_2001.htm (accessed 27 Jan. 2007).

2. James A. Johnson, "A Brief History of Terrorism," in *Community Preparedness and Response to Terrorism,* Volume 1, *The Terrorist Threat and Community Response*, ed. Gerald R. Ledlow, James A. Johnson, and Walter J. Jones (Westport, CT: Praeger), p. 2.

3. W. Timothy Coombs, "The Terrorist Threat: Shifts in Crisis-Management Thinking and Planning Post-9/11," in *Community Preparedness and Response to Terrorism,* Volume 3, *Communication and the Media*, ed. H. Dan O'Hair, Robert L. Heath, and Gerald R. Ledlow (Westport, CT: Praeger), pp. 214–215.

4. G. Andrew Karolyi and Rodolfo Martelli, "Terrorism and the Stock Market," Nov. 2005, online at http://www.cob.ohio-state.edu/fin/dice/papers/2005/2005-19.pdf (accessed 27 Jan. 2007).

ECOTERRORISM

W. Timothy Coombs

Some terrorism is based on what a company does rather than just the political goals of the terrorist organization. Ecoterrorism targets corporations at odds with the environmental concerns of the terrorist group. The FBI defines ecoterrorism as "the use or threatened use of violence of a criminal nature against innocent victims or property by an environmentally-oriented, subnational group for environmental-political reasons, or aimed at an audience beyond the target, often of a symbolic nature."[1] If your company has some involvement with environmental issues related to the concerns of an ecoterrorism group, it should be prepared to manage that risk.

Ecoterrorists see themselves as protecting the earth. They engage in crimes they believe are designed to save the planet. Their direct actions attempt to avoid human injuries. This statement from the Animal Liberation Front (ALF) reveals its target and vows not to harm humans:

> Animal Liberation Front Guidelines
>
> 1. To liberate animals from places of abuse, i.e., fur farms, laboratories, factory farms, etc., and place them in good homes where they may live out their natural lives free from suffering.
> 2. To inflict economic damage to those who profit from the misery and exploitation of animals.
> 3. To reveal the horror and atrocities committed against animals behind locked doors by performing nonviolent direct actions and liberations.
> 4. To take all necessary precautions against hurting any animal, human and non-human.
>
> In the third section it is important to note the ALF does not, in any way, condone violence against any animal, human or non-human. Any action involving violence is by its definition not an ALF action, and any person involved is not an ALF member.
>
> The fourth section must be strictly adhered to. In over 20 years, and thousands of actions, nobody has ever been injured or killed in an ALF action.[2]

However, in the United States, ecoterrorism is defined by law enforcement as terrorism, and groups engaging in ecoterrorism are considered domestic terror groups. Here's a sample of Earth Liberation Front (ELF) corporate attacks since 1997:

March 14, 1997. Near Eugene, Oregon. Tree spiking at Robinson-Scott timber harvest site in the Mackenzie River watershed, Willamette National Forest.

July 21, 1997. Redmond, Oregon. Fire at the Cavel West meat packing plant in Redmond. Estimated cost over $1 million.

October 19, 1998. Vail, Colorado. Fires burns part of the Vail ski resort; seven structures destroyed: four ski lifts, a restaurant, a picnic facility, and a utility building. Damages: $12 million.

October 26, 1998. Powers, Michigan. Release of 5,000 mink at Tom Pipkorn's Mink Farm near Hermansville. Damages: $100,000.

December 27, 1998. Medford, Oregon. Fire at the headquarters of U.S. Forest Industries. Damages: $500,000.

December 25, 1999. Monmouth, Oregon. Fire burns down a Boise Cascade timber management office. Damages: $1 million.

December 31, 1999. Lansing, Michigan. Arson breaks out in the offices of Catherine Ives, Room 324, Michigan State University's Agriculture Hall, a campus landmark. The office is connected to genetically modified crop research for Monsanto. Graffiti and damage amount to around $400,000.

November 27, 2000. Niwot, Colorado. Arson fire burns one of the first luxury homes going up in a new subdivision. Damages: $500,000.

December 30, 2000. Mount Sinai, New York. Three luxury homes under construction are burned and a fourth is spray-painted with graffiti. Damages: $160,000.

January 2, 2001. Glendale, Oregon. Arson at the offices of Superior Lumber Company, the town's leading employer. Damages: $400,000.

August 22, 2003. East Suburban Los Angeles, California. Arsonists attack several car dealerships in east suburban Los Angeles, burning down a warehouse and vandalizing several cars. All told, more than 100 cars are damaged or destroyed. Damages: over $1,000,000.[3]

If your company fits with any of the past ELF or other ecoterrorist targets, it is a potential future target for ecoterrorism.

Earth First! is a third well-known ecoterrorist group that started in the United States and has now spread to the United Kingdom. Earth First! uses a mix of nonviolent and violent methods as ecodefense (strategies to defend the environment). Its violent methods are termed monkeywrenching, which can include arson, tree spiking, billboard vandalism, road reclamation, and ecotage (eco-sabotage). Tree spiking is an especially dangerous form of monkeywrenching. Ecoterrorists spike trees by driving metal rods or other materials into the tree trunk. The danger is that if a metal saw blade hits a spike, the blade will break or shatter. A shattering blade can injure workers, either loggers felling the trees or people in the sawmills. Spikes are placed high so that loggers will not hit them and trees are marked so that they will not be used. Spiking significantly reduces the economic value of a tree. Still, a spiked tree does create the potential for injury. Tree spiking became a federal felony in 1988 and Earth First! did renounce its use in 1990. However, you can still find references to this practice on its web site.

One way to prepare for ecoterrorism is to learn more about these groups. By studying them, you can determine whether your company is a potential target and learn their attack strategies. You can easily find the web sites for ELF, ALF, and Earth First! on the Internet; and books about ecoterrorists, such as Dave Foreman's *Ecodefense: A Field Guide to Monkeywrenching,* are also useful.

The Ozymandias Sabotage Handbook is an online guide to ecoterrorism. Here is an excerpt on quarry attacks:

> There are four key targets in the quarry works:
>
> - The earth moving/excavation equipment.
> - The pumps that keep the quarry dry—if you are certain the site will fill with water quickly, or you can swap the pipes on the pumps, then you can drown all the equipment in one go.

- The sorting/grading and crushing equipment—essential for the processing of stone, and potentially easily damaged.
- The site office and weighbridge. Doing the site office causes annoyance. If you can damage the controls for the weighbridge then you really make operating difficult.[4]

CONCLUSION

Ecoterrorists are not to be taken lightly because they pose a threat to an organization's operation and profitability. ALF, for example, is responsible for the elimination of many research projects. It also claims to be the cause of increased spending for security by research laboratories. Ecoterrorism is a real threat for any company whose actions touch the agenda of radical environmental groups. Organizations are right to increase security for ecoterrorists. The ecoterrorist guides indicate potential targets at facilities and how best to attack the targets. The guides also cover topics such as planning an attack and how to avoid detection. An analysis of these guides can help to prevent attacks by understanding the targets and methods of attack. You can better prepare a defense when you know how your enemy operates.

See also Countersurveillance; and Terrorism.

NOTES

1. James F. Jarboe, "The Threat of Eco-Terrorism," 12 Feb. 2002, online at http://www.fbi.gov/congress/congress02/jarboe021202.htm (accessed 29 Jan. 2007).

2. Animal Liberation Front, "The ALF Primer," 1991, online at http://www.animalliberationfront.com/ALFront/ALFPrime.htm (accessed 29 Jan. 2007).

3. Center for the Defense of Free Enterprise, "Earth Liberation Front," online at http://www.cdfe.org/elf.htm (accessed 28 Jan. 2007).

4. "Ozymandias Sabotage Handbook," online at http://www.reachoutpub.com/osh/ (accessed 29 Jan. 2007).

AGROTERRORISM

W. Timothy Coombs

Agroterrorism refers to terrorist attacks on agricultural targets. Companies involved in any aspect of the farm-to-table chain should build defenses against agroterrorism into their business security and crisis management plans. These include companies involved in crops, livestock, distribution, processing, retail, transportation, and storage. Agroterrorism is a serious concern because such attacks could harm or kill a large number of people. In addition, an agroterrorism attack would severely impact the economy through lost wages, health care costs, and loss of business. Agroterrorism is part of the Bioterrrorism Preparedness and Response Act of 2002.

Agroterrorism is concerned with food security rather than food safety. Food safety focuses on efforts to prevent the unintentional contamination of food. *E. coli* outbreaks due to improperly prepared ground beef or vegetables contaminated by groundwater are examples of food safety. Food security guards against intentional acts of contamination or tampering. Refer to the Food Tampering box for examples of agroterrorism. Although it is a heightened concern after the 9/11 attacks, food tampering has always been a risk that companies in the agricultural industry have had to face. The incidents of product tampering are rare but they are a known risk. Evidence of concern over food tampering is found in the various tamper-resistant packaging encountered every day. Before using the peanut

Food Tampering

Here are some incidents of attacks on the food supply in the United States.

In 1984, in Oregon, members of cult led by Bhagwan Shree Rajneesh contaminated a restaurant salad bar with cultivated *Salmonella* bacteria. The goal was to affect a local election. No one died but there were approximately forty-five individuals needing hospitalization. Local public health officials detected the outbreak, but it took the FBI an entire year to connect the outbreak to the cult.

In 1996, a laboratory employee contaminated a tray of doughnuts and muffins with the food-borne pathogen *Shigella dysenteriae* Type 2. The employee sent an e-mail invitation to forty-five employees, using an unoccupied supervisor's computer, to have pastries in the employee break room. Twelve of the forty-five employees did eat some amount of a pastry and contracted a severe gastrointestinal illness. Four of those employees had to be hospitalized, but no one died. The pathogen was from that laboratory. The employee had exploited lax security to access the pathogen.

In 2003, a Michigan supermarket employee used a nicotine-based pesticide to contaminate 200 pounds of ground beef. The official count from the CDC identified 92 individuals who had become ill from consuming the ground beef. The Michigan case illustrates how easy it is for just one person to contaminate the food supply intentionally and have a serious impact.

Notice that the attacks are low in death (mortality) but high in illness (morbidity). However, deaths could increase if more deadly pathogens were used.[1]

butter, for example, you need to remove the inside cover, and you need to be sure the seal is intact on plastic beverage bottles.

EFFECTS OF AGROTERRORISM

Consider this statistic: Over 76 million illnesses, 325,000 hospitalizations, and 5,000 deaths each year are attributed to the unintentional contamination of the food supply.[2] That number could be much higher if terrorists decided to target the food supply aggressively. The food safety data reveal the weaknesses in the farm-to-table chain. Food safety incidents show the types of foods and points in their production where intentional contamination could occur. It is logical that a terrorist would use naturally occurring vulnerabilities for an attack. Hence, some lessons from food safety are applicable to food security.

The economic effect of an intentional attack is potentially very serious. People will be afraid to consume certain foods resulting in loss of revenue. This is akin to restaurant chains that see a drop in business following a food-borne illness outbreak such as the 2006 *E. coli* incident at Taco Bell.

The Chilean fruit case is a further illustration of the impact of agroterrorism. In 1989, a terrorist organization phoned the U.S. Embassy in Chile claming to have used cyanide to contaminate Chilean grapes. The Food and Drug Administration (FDA) carefully monitored the situation. It identified only three suspicious grapes at a Philadelphia, Pennsylvania, dock. Across the United States, supermarkets removed Chilean fruit from their shelves, and U.S. consumers were warned not to eat Chilean fruit. At that time of year, most of the blueberries, peaches, melons, pears, green apples, blackberries, and plums were imported from Chile. The lost revenue totaled over $200 million. Consumer confidence in Chilean fruit was slow to recover.[3]

Agroterrorism can have economic, health, societal, psychological, and political consequences. Widespread public fear accompanies any deliberate food contamination. People become ill and then lose confidence in food supply safety and the effectiveness of the government. Let us examine the economic effect more closely. Breaches in food security can result in health care expenses, lost wages, damaged consumer confidence, trade embargoes, and the like. The Centers for Disease Control (CDC) divides the economic effects of agroterrorism into three categories:

1. *Direct economic* losses attributable to responding to the act, including medical costs, lost wages for the victims, containment, decontamination, and disposal costs
2. *Indirect multiplier effects* from compensation paid to affected producers and the losses suffered by affiliated industries, such as suppliers, transporters, distributors, and so on
3. *International costs* in the form of trade embargoes imposed by trading partners.[4]

AGROTERRORISM VULNERABILITIES

Vulnerabilities are the areas of weakness at which the risk is greatest for incidents to occur. The Food and Drug Administration (FDA) and U.S. Department of Agriculture (USDA) vulnerability assessments have found these four principal factors for agroterrorism risk:

1. Food prepared in large batches, such as shredded lettuce. With large batches comes the ability to reach an increased number of potential consumers with one tampering effort. The more people that are exposed, the greater the damage from morbidity/mortality, economic impact, and fear. Which has the greater impact, 5,000 pounds or 50 pounds of ground beef?
2. Food with a short shelf life and/or rapid turnaround at retail outlets and quick consumption. Public health officials have little time to identify a problem and take action when there is rapid turnaround and consumption of a contaminated product. Examples would be highly perishable products such as bread, milk, and fresh ground meat. These types of products are generally consumed within a few days to a little over a week.
3. Food that involves uniform mixing. A terrorist would add the contaminant before or during the uniform mixing process. The attack would be more potent as all servings from the batch would be contaminated. Not all uniform mixing processes are equal in spreading a contaminant equally throughout a batch. The best target would be some nonviscous fluids, such as milk and liquid eggs, and in processes wherein the equipment is designed to ensure thorough mixing. Some mixing processes, including grain and corn syrup, resist mixing and will not allow a contaminant to be spread throughout the batch.
4. Ease of access to the product or process is the final factor. The value of a target increases with the ease of access. A terrorist must have access to introduce the contaminant. How easy is it for people, including workers, to access critical areas of your company?[5]

In addition to the four principal factors, certain additional features of a product make it more or less attractive as an agroterrorism target. These factors include ability to hide the contaminant, attractiveness of target, tamper-evident packaging, and serving size. Ideally the contaminant can be disguised in the food. Some foods make better targets because they exhibit a strong flavor (e.g., spaghetti sauce), odor (e.g., fish sauce), or texture (e.g., ground meat); intense color (e.g., soy sauce); or opaqueness (e.g., chocolate syrup). Such attributes serve to conceal the contaminant, especially a contaminant that has a flavor or odor than might alert people to its presence.[6]

Food that lacks tamper-evident packaging or other wrapping that reduces the potential for the product to be tampered with or counterfeited increases the risk of intentional contamination. Young children and the elderly are desirable targets. Due to health issues and body weight, these two populations are more likely to be seriously affected by small dosages. This is similar to how children are at greater risk of serious illness or death from *E. coli* than is the average adult. Moreover, children as a target increase public concern and media attention to the contamination. Finally, food that has small servings is less attractive because it is difficult to deliver a lethal or damaging dose of the contaminant.

A variety of contaminants can be used including chemical, biological, and radiological. The contaminating agent could be natural, one that is found in unintentional contamination of the food such as *E. coli*. Or an agent could be "exotic," such as those found in biological or chemical warfare.

The attitude of your employees is another vulnerability factor. Workers become lax when they think intentional contamination would never happen at their facility. Employees need to combat apathy about food security. As the government's food security training program notes, "Lack of knowledge about food security and a lack of commitment to food security may also hamper employees. It is important to educate employees about the fundamental principles and importance of food security and let them know that the typical aggressor thrives on their lack of vigilance."[7]

ANATOMY OF AN AGROTERRORISM EVENT

A successful tampering of food products requires three elements: The perpetrator must (1) have access for a sufficient period of time, (2) have the technical knowledge to obtain or produce and to introduce a sufficient quantity of the contaminant, and (3) be able to contaminate the food without detection. In short, a perpetrator needs the desire, appropriate skills and materials, and ability for an effective attack. The perpetrator must know the food's farm-to-table chain and have the competence to plan an attack that will allow the contaminant to avoid detection or ensure the contaminant will not be eliminated in the manufacturing, distribution, and consumption process.

POTENTIAL AGROTERRORISTS

The government divides those who would contaminate the food supply into four groups:

1. *Disgruntled insiders* are generally motivated by their own emotions and self-interests. They may be mentally unstable, operating impulsively with minimal planning. This may be the most difficult group to stop because they may have legitimate access to the product.
2. *Criminals* who are sophisticated may possess relatively refined skills and tools and are generally interested in high-value targets. Unsophisticated criminals have more crude skills and tools and typically have no formal

organization. They are generally interested in targets that pose a low risk of detection.

3. *Protesters* are usually politically or issue oriented. They generally act out of frustration, discontent, or anger. They are primarily interested in publicity for their cause and, as a result, generally do not intend to injure people, but may be superficially destructive. They are usually unsophisticated in their tactics and planning. However, some protest groups have adapted tactics similar to terrorists. In this way, they may be moderately sophisticated and moderately destructive. In fact, they may target individuals for harm.
4. *Terrorists* are usually politically or ideologically oriented. They typically work in small, well-organized groups and are typically well funded, sophisticated, and capable of efficient planning. Terrorists may use other types of aggressors to accomplish their goals. Their objectives include death, destruction, theft, and publicity.[8]

Another way of looking at potential attackers is dividing them by the nature of an attack: internal or external. Internal attacks can be conducted by disgruntled employees, cleaning crews, contractors, temporary employees, or members of a terrorist group posing as employees. External attacks can come from terrorist groups, activist groups, truck drivers (shipping and receiving), contractors, suspect suppliers, and visitors.

TYPES OF AGROTERRORIST ATTACKS

The government has identified four basic types of attacks: insider compromise, exterior attack, forced entry, and covert entry.

- Insider compromise occurs when the attacker uses his or her legitimate access to the food (e.g., as an employee) to contaminate it.
- Exterior attack involves the aggressor contaminating a raw material (e.g., an ingredient used in the food production process) at a point where it is grown, transported, or processed. The contaminated raw material then enters the food processing facility through a normal channel. Attackers can also steal shipments and sell them on the black market to raise money. Subverting shipments of legitimate product for black-market moneymaking schemes is another form of exterior attack. In addition to raising money, the product can also be tampered with, providing another avenue for the contamination to enter the market.
- Forced entry occurs when an attacker illegally enters a facility in order to contaminate the food. The aggressor must be able to force entry without being detected. Diversions, such as vandalism or theft, can be used to mask a forced entry.

- Covert entry is when an attack uses deception of employees or stealth to gain entry to a facility. Covert entry can be viewed as a form of social engineering. For instance, an attacker may enter as a member of a tour group or even impersonate a government employee.[9]

DEFENDING AGAINST AGROTERRORISM

Begin dealing with the threat of agroterrorism by conducting a vulnerability audit. The Food Safety Inspection Service recommends two methodologies: the ORM and Carver + Shock. These two methodologies, outlined below, are not the only vulnerability assessment methodologies but are noted by the U.S. government.

ORM

A defensive vulnerability assessment tool to identify points in a system that are most susceptible to terrorist attack and design preventive measures to reduce risk. ORM considers two factors that affect the risk of attack at a particular point:

1. Severity – Public health impacts of an attack
2. Probability – Likelihood that an attack could occur

Carver + Shock

An offensive target prioritization tool to identify critical nodes most likely to be targets of terrorist attack and design preventive measures to reduce risk. CARVER + Shock considers seven factors that affect the attractiveness of a target:

- Criticality – Degree to which the public health and economic impacts achieve the attacker's intent
- Accessibility – Physical access to a target
- Recuperability – Ability of the system to recover from an attack
- Vulnerability – Ease of accomplishing an attack
- Effect – Amount of direct loss from an attack
- Recognizability – Ease of identifying a target
- Shock – Psychological effects of an attack[10]

CONCLUSION

Once the vulnerabilities are understood, a company can begin to develop a food security plan. Refer to the Food Security entry for a more detailed discussion of the topic. A key ingredient in any agroterrorism prevention is awareness and vigilance by your employees. Management must have a program for communicating and reinforcing the value of food security to employees. Food security needs to be a regular topic of conversation in the company, not a just a random note in an e-mail. Employees must be encouraged to report possible tampering, suspicious activities, and any weaknesses they see in security. Employees are on the front-lines of agroterrorism. Vigilant employees are one of the best ways to detect and to respond to intentional contamination.

See also Food Security; Strategic Partnership Program Agroterrorism; Supply Chain Security; and Terrorism.

NOTES

1. U.S. Food and Drug Administration, "Food Security Awareness: Intentional Contamination," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/7.html (accessed 28 Jan. 2007).

2. Centers for Disease Control and Prevention, "Final FY 2003 GPRA Annual Performance Plan Revised Final FY 2002 GPRA Annual Performance Plan FY 2001 GPRA Annual Performance Report," Feb. 2002, online at http://0-www.cdc.gov.mill1.sjlibrary.org/od/perfplan/2002/2002perf.pdf (accessed 28 Jan. 2007), p. 13.

3. U.S. Food and Drug Administration, "Food Security Awareness: Threats as Weapons," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/8.html (accessed 28 Jan. 2007).

4. U.S. Food and Drug Administration, "Food Security Awareness: Reasons to Attack the Food Supply," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/9.html (accessed 28 Jan. 2007).

5. U.S. Food and Drug Administration, "Food Security Awareness: High Risk Attributes of Food," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/10.html (accessed 28 Jan. 2007).

6. U.S. Food and Drug Administration, "Food Security Awareness: High Risk Attributes of Food," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/12.html (accessed 28 Jan. 2007).

7. U.S. Food and Drug Administration, "Food Security Awareness: Attitudes of Employees," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/15.html (accessed 28 Jan. 2007).

8. U.S. Food and Drug Administration, "Food Security Awareness: Types of Aggressors," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/17.html (accessed 28 Jan. 2007).

9. U.S. Food and Drug Administration, "Food Security Awareness: Tactics of Aggressors," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/19.html (accessed 28 Jan. 2007).

10. U.S. Food and Drug Administration, "Food Security Awareness: Preventative Measures General," online at http://www.fda.gov/ora/training/orau/FoodSecurity/textpages/20.html (accessed 28 Jan. 2007).

STRATEGIC PARTNERSHIP PROGRAM AGROTERRORISM (SPPA)

W. Timothy Coombs

The Strategic Partnership Program Agroterrorism (SPPA) is a collaborative initiative designed to protect the food supply of the United States. The collaboration includes the Department of Homeland Security (DHS), U.S. Department of Agriculture (USDA), Food and Drug Administration (FDA), and Federal Bureau of Investigation (FBI), along with private industry, trade associations, and the states.[1] According to the SPPA web site, the program's objectives are as follows:

- Validate or identify sector-wide vulnerabilities by conducting critical infrastructure/key resources (CI/KR) assessments in order to:
  a. Identify gaps;
  b. Inform Centers of Excellence and Sector Specific Agencies (SSA) of identified research needs; and
  c. Catalog lessons learned.
- Identify indicators and warnings that could signify planning for an attack.
- Develop mitigation strategies to reduce the threat/prevent an attack. Strategies may include actions that either industry or government may take to reduce vulnerabilities.
- Validate assessments conducted by the United States Government (USG) for food and agriculture sectors.
- Gather information to enhance existing tools that both USG and industry employ.
- Provide the USG and the industry with comprehensive reports including warnings and indicators, key vulnerabilities, and potential mitigation strategies.
- Provide sub-sector reports for the USG that combine assessment results to determine national critical infrastructure vulnerability points to support the National Infrastructure Protection Plan (NIPP) and national preparedness goals.
- Establish and/or strengthen relationships between Federal, State, and local law enforcement and the food and agriculture industry along with the critical food/agriculture sites visited.[2]

The focal point of SPPA is to conduct vulnerability assessments of the food and agriculture sector. SPPA teams visit a number of sites and help to perform the audits as the initial step for improving food security. These assessments create an understanding of industry-wide as well as facility-specific vulnerabilities.

The industry-wide vulnerabilities create targeted areas that all facilities should consider and that the SPPA should highlight for greater attention. Moreover, a facility learns specific vulnerabilities it can improve and learns what others have been doing to mitigate security threats. The SPPA also provides tools for facilities wishing to conduct their own vulnerability assessments/audits.

The SPPA touches a wide range of agro-businesses. The list includes the following: aquaculture production facilities, beef cattle feedlots, cattle stockyards/auction barns, citrus production facilities, corn farms, dairy farms, grain elevators and storage facilities, grain export handling facilities, poultry farms, rice mills, seed production facilities, soybean farms, swine production facilities, veterinary biological firms, deli meat processing, ground beef processing facilities, hot dog processing, import reinspection facilities, liquid egg processing, poultry processing, retailers, school food service central kitchens, transportation companies, warehouses, animal food/feeds, baby food, bread foods (frozen and raw), canned food, cereals, deli salads, dietary supplements, fully cooked entrees, flour, frozen packaged entrees, fruit juice, gum Arabic, high fructose corn syrup, honey, ice cream, infant formula, milk (fluid), peanut butter, produce (fresh, cut, and retail setting), seafood (cooked, refrigerated, and ready-to-eat), carbonated soft drinks, vitamins (capsules and premixes), bottled water, and yogurt.

CONCLUSION

The SPPA can touch upon a large number of industries, so companies should take the time to learn more about this food security group. SPPA could prove valuable to small agro-businesses looking to improve security.

See also Agroterrorism.

NOTES

1. U.S. Food and Drug Administration, “SPPA Questions and Answers,” 23 Sept. 2005, online at http://www.cfsan.fda.gov/~dms/agroter4.html (accessed 28 Jan. 2007).

2. U.S. Food and Drug Administration, “Executive Summary,” Aug. 2005, online at http://www.cfsan.fda.gov/~dms/agroterr.html (accessed 28 Jan. 2007).

FOOD SECURITY

W. Timothy Coombs

Like other business security issues, the need for food security existed before the attacks of 9/11. For companies involved in the processing, transportation, or storage of food, a food security plan has always been valuable. Two current factors are reinforcing its value. First, the food sector has been listed as a possible terrorist target (agroterrorism), increasing the value of a food security plan. Second, government programs, such as the USDA's Agriculture Marketing Service (AMS), are building food security requirements into their contract specifications. The Food Safety Inspection Service (FSIS) has resources to help small and very small companies address food security issues. The FSIS provides model plans for a variety of food industry establishments that can be adapted to fit the security and budgetary needs of a company.

The FSIS food security plans are built on five principles of food security.

- *Principle 1: Clearly understand what needs to be protected.* Companies must conduct a vulnerability/food security assessment. Such assessments identify where the greatest threat lies and where the company needs to focus its protective efforts.
- *Principle 2: Apply the highest security to the most critical components.* The security measures need to match the demands of the vulnerability and threat. The most critical systems and those with the greater probability of attack and greatest potential to inflict harm should receive greatest protection.
- *Principle 3*: *Employ a layer approach.* Facility security is a combination of multiple overlapping approaches including physical security, personnel security, and operational security. Consider a layered approach to security. On the outside is access control. The next layer is screening and training employees about food security. Inside are the processes and procedures that should reduce operational risk.
- *Principle 4: Reduce risk to an acceptable level.* Food security risks cannot be reduced to zero. Such a level is neither possible nor financially viable. Companies must consider the cost-benefit ratio when addressing countermeasures for food security.
- *Principle 5*: *Security must have strong management support.* No change in an organization survives without strong support from top management. Employees will let time pressures and budgets kill a change if management does not support and reinforce the change. Management must show a real commitment to food security.[1]

The FSIS recommends a three-step planning process: (1) conduct a food security assessment, (2) develop a food security plan, and (3) implement the plan. The first step requires that a company understand its vulnerabilities in order to develop countermeasures. The FSIS has an Industry Self-Assessment Checklist for Food Security and other vulnerability assessment tools. The Guidance Appendix provides samples of FSIS assessment tools.

The development of a food security plan is built around five food security goals:

1. *Ensure inside security.* This includes visitor access to designated areas in a facility, protection of critical plant systems such as airflow and water, and supervision and screening of contract workers that are given access to your facility.
2. *Ensure processing security.* The equipment used in the process, raw materials, and finished products must be monitored. It also includes personnel security for employees.
3. *Ensure storage security.* Storage areas must be secured and monitored. The company must control access to ingredient and product storage areas. This includes keeping strict maintenance records.
4. *Ensure general outside security.* The company must try to prevent access by unauthorized intruders. This involves perimeter control (e.g., fencings, gates, guard stations, and key card access), securing all entry points, and using exterior lighting and closed circuit cameras.
5. *Ensure shipping and receiving security.* The company must make sure the raw materials coming in and finished products leaving a facility are secure. Vendors must be screened, incoming deliveries controlled, raw materials inspected, drive access limited during deliveries, and tamper-evident seals used on incoming and outgoing shipments.

The Food Security Plan Table provides sample vulnerabilities and potential security measures for each of the five goals.

Vulnerabilities	Potential Security Measures
Access to exterior of a facility	Proper lighting and alarms Fences and gated entries
Access to vehicles	Locks, seals, or sensors on trucks and railcars Outgoing shipments have tamper-evident seals
Visitors on site	System to identify and monitor visitors
Access inside facility	Proper lighting and CCTV surveillance Key inventories Limited access to clearly marked restricted areas
Access to critical components	Restricted access to heating, cooling, ventilation, electrical, gas, and disinfection systems
Access to storage facilities	Controlled and restricted access including carefully maintained logs
Access to hazardous materials	Regularly inventoried with restricted access

CONCLUSION

The implementation of the food security plan involves assigning responsibilities for various parts of the plan, training employees to use the plan, conducting drills to test the plan, and revising the plan. The food security plan is a living document that needs regular updating and testing.

See also Agroterrorism; Physical Security; Strategic Partnership Program Agroterrorism; and Terrorism.

NOTE

1. "Food Security: Make It Your Business," July 2005, online at http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Workshop_Food_Security/index.asp (accessed 28 Jan. 2007).

TERRORISM AND CHEMICAL FACILITIES

W. Timothy Coombs

The Environmental Protection Agency (EPA) estimates there are 110 chemical facilities in 22 states in the United States that could affect over 1 million people with a toxic release. Facilities in 44 states could affect populations of over 100,000 people.

A chemical facility is any plant or warehouse where chemicals are used, manufactured, or stored. Chemical facilities are attractive targets for terrorists because these facilities could act as weapons of mass destruction. Attacks on chemical facilities could generate serious collateral damage among people living near a facility.[1] Most chemical facilities already have emergency plans in place and systems for warning nearly every residence to evacuate or to shelter-in-place. These emergency plans were developed for unintentional chemical releases.

Terrorism raises the specter of intentional attacks on chemical facilities. Following the 9/11 attacks, industry leaders and politicians preached the need to improve security around chemical facilities. The news show *60 Minutes* was one of many media outlets that ran a dramatic piece showing how easy it is to breach perimeter security at some chemical facilities. The media may have overstated the problem, but it drew attention to the need to strengthen perimeter and other security at chemical facilities.

INDUSTRY ACTIONS

The American Chemistry Council (ACC) has been the industry leader in improving security. The ACC members represent about 85 percent of all the chemicals produced in the United States. Following the attacks of 9/11, the ACC adopted a plan for improving security known as the Responsible Care© Security Code (RCSC). According to ACC data, its membership is complying. The first stage of RCSC was to complete a security vulnerability assessment. A total of 99.58 percent of the membership completed the security vulnerability assessment on time. The remaining members completed the evaluation within 60 days of the deadline, meaning over 2,000 facilities have completed the assessment. The Responsible Care companies had to implement any physical security enhancements revealed by their vulnerability assessments by December 31, 2004. The program called for additional security safeguards deemed necessary in the assessment to be put in place and then independently verified by third parties. A total of 94.75 percent of the Responsible Care facilities had their third-party assessments completed on time. That compliance rate had reached 99.63 percent by the end of 2005. The ACC was still compiling the final implementation statistics in early 2007.[2]

GOVERNMENTAL ACTIONS

The federal government took action in 2006 with H.R. 5441, the Department of Homeland Security Appropriations Act, 2007. One of the many provisions in this bill gave formal authority to DHS to set national chemical security performance standards, to inspect chemical facilities, and to penalize those who do not comply. Here is the exact wording of the bill:

> SEC. 550. (a) No later than six months after the date of enactment of this Act, the Secretary of Homeland Security shall issue interim final regulations establishing risk-based performance standards for security of chemical facilities and requiring vulnerability assessments and the development and implementation of site security plans for chemical facilities: *Provided,* That such regulations shall apply to chemical facilities that, in the discretion of the Secretary, present high levels of security risk: *Provided further,* That such regulations shall permit each such facility, in developing and implementing site security plans, to select layered security measures that, in combination, appropriately address the vulnerability assessment and the risk-based performance standards for security for the facility: *Provided further,* That the Secretary may not

(continued)

disapprove a site security plan submitted under this section based on the presence or absence of a particular security measure, but the Secretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section: *Provided further,* That the Secretary may approve alternative security programs established by private sector entities, Federal, State, or local authorities, or other applicable laws if the Secretary determines that the requirements of such programs meet the requirements of this section and the interim regulations: *Provided further,* That the Secretary shall review and approve each vulnerability assessment and site security plan required under this section: *Provided further,* That the Secretary shall not apply regulations issued pursuant to this section to facilities regulated pursuant to the Maritime Transportation Security Act of 2002, Public Law 107-295, as amended; Public Water Systems, as defined by section 1401 of the Safe Drinking Water Act, Public Law 93-523, as amended; Treatment Works as defined in section 212 of the Federal Water Pollution Control Act, Public Law 92-500, as amended; any facility owned or operated by the Department of Defense or the Department of Energy, or any facility subject to regulation by the Nuclear Regulatory Commission.

(b) Interim regulations issued under this section shall apply until the effective date of interim or final regulations promulgated under other laws that establish requirements and standards referred to in subsection (a) and expressly supersede this section: *Provided,* That the authority provided by this section shall terminate three years after the date of enactment of this Act.

(c) Notwithstanding any other provision of law and subsection (b), information developed under this section, including vulnerability assessments, site security plans, and other security related information, records, and documents shall be given protections from public disclosure consistent with similar information developed by chemical facilities subject to regulation under section 70103 of title 46, United States Code: *Provided,* That this subsection does not prohibit the sharing of such information, as the Secretary deems appropriate, with State and local government officials possessing the necessary security clearances, including law enforcement officials and first responders, for the purpose of carrying out this section, provided that such information may not be disclosed pursuant to any State or local law: *Provided further,* That in any

(continued)

proceeding to enforce this section, vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this section, and related vulnerability or security information, shall be treated as if the information were classified material.

(d) Any person who violates an order issued under this section shall be liable for a civil penalty under section 70119(a) of title 46, United States Code: *Provided,* That nothing in this section confers upon any person except the Secretary a right of action against an owner or operator of a chemical facility to enforce any provision of this section.

(e) The Secretary of Homeland Security shall audit and inspect chemical facilities for the purposes of determining compliance with the regulations issued pursuant to this section.

(f) Nothing in this section shall be construed to supersede, amend, alter, or affect any Federal law that regulates the manufacture, distribution in commerce, use, sale, other treatment, or disposal of chemical substances or mixtures.

(g) If the Secretary determines that a chemical facility is not in compliance with this section, the Secretary shall provide the owner or operator with written notification (including a clear explanation of deficiencies in the vulnerability assessment and site security plan) and opportunity for consultation, and issue an order to comply by such date as the Secretary determines to be appropriate under the circumstances: *Provided*, That if the owner or operator continues to be in noncompliance, the Secretary may issue an order for the facility to cease operation, until the owner or operator complies with the order.[3]

The ACC supported this legislation and has worked with the DHS since its inception to address concerns over chemical facility safety. Now all chemical facilities that qualify will be under some security control by the DHS. Small facilities that pose minimal risks and are low-probability targets are exempt from DHS supervision. On December 22, 2006, the DHS placed a set of regulations designed to improve security at high-risk chemical facilities on display for public comment. The regulations in this document will guide future security efforts at chemical facilities. DHS uses four points to establish high risk: (1) consequences of a release including size of the population that could be affected, (2) threat presented by sabotage of products, (3) potential harm from stolen products, and (4) economic and national security effects of an attack.

CONCLUSION

Since 2003, many chemical facilities have been actively improving physical and information security using the RCSC guidelines. The DHS will recognize alternative security programs as compliance with DHS standards, and the RCSC is one that is being considered.[4] Even if the RCSC is accepted as an alternative security program, security personnel at chemical facilities will need to integrate DHS requirements into their current and future security efforts.

See also Physical Security; and Terrorism.

NOTES

1. "Planning for the Worst," *Contingency Planning Management*, 6, 5 (2001), 16.
2. Scott Jensen and Ben Zingman, "The Race for Chemical Security," *American Chemistry*, March/April 2007, p. 31.
3. George W. Bush, "President's Statement on H.R. 5441, the "Department of Homeland Security Appropriations Act, 2007," 4 Oct. 2006, online at http://www.whitehouse.gov/news/releases/2006/10/20061004-10.html (accessed 12 Feb. 2007).
4. American Chemistry Council, "Chemical Industry Security," 2007, online at http://reporting.responsiblecare-us.com/reports/fclty_ia_rpt.aspx (accessed 12 Feb. 2007).

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

W. Timothy Coombs

Following the 9/11 attacks, the U.S. Customs and Border Protection (CBP) was challenged to create a system to secure supply chains that then spanned the globe. The program needed to reduce the threat of terrorism while also facilitating the speed of international trade. The end result was the Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary partnership between the private and public sectors. It is not a simple process, but the C-TPAT Benefits box cites reasons why businesses would want to sign on to C-TPAT.

The government works with businesses that cooperate with one another to develop the criteria necessary to validate the safety of the supply chain. Private partners document and validate that their supply chain meets the relevant criteria or guidelines developed by C-TPAT. The private partners develop an internal validation process to document their efforts to secure their supply chain. Government representatives use the internal validation information as part of their efforts to validate each private partner's security efforts. Validation is based

C-TPAT Benefits

The benefits of C-TPAT membership include the following:

1. Reduce the number of inspections and reduce waiting times at the border.
2. C-TPAT can help businesses with validation, training, and security issues.
3. C-TPAT members can access the Status Verification interface.
4. There are self-policing and self-monitoring of security activities.
5. Exclusion from certain trade-related local and national criteria.
6. Importers receive targeting benefits.
7. Eligible for FAST lanes on Canadian and Mexican borders.
8. Eligible for the Importer Self-Assessment Program (ISA).
9. Can attend C-TPAT supply chain security training seminars.
10. Improve your organization's logistical security.
11. Greater mitigation of risk.
12. Reduced cargo theft.

upon the unique security factors faced by the private partner including geographic areas of operation, volume of trade, and security-related anomalies. Government officials seek to document whether the required security procedures are being used to meet C-TPAT guidelines or criteria. C-TPAT is an evolving process. As new risks, technologies, and security knowledge emerge, the criteria for C-TPAT validation change. An example of that are the 2006 updates to C-TPAT validation criteria for customs brokers.

The C-TPAT security criteria cover areas such as business partner requirements, conveyance tracking and monitoring, physical access controls, personnel security, procedural security, documentation processing, physical security, information technology security, and security training and threat awareness. The range of concerns reflects the need to integrate physical and information security. Business partner requirements focus on gathering written and verifiable screening of new business partners. The key is to document that the business partners are following the C-TPAT criteria or guidelines for security. Conveyance tracking and monitoring procedures include seals used to ensure a cargo's integrity and the ability of an organization to track and to monitor the movement of cargo containers.

Physical access controls seek to keep unauthorized personnel away from cargo during its movement through the supply chain whether at rest or in transit. The focus is on control of employees and visitors. This includes employee identification, restricting access to vendors and visitors, and determining unauthorized persons. Personnel security involves following proper screening of employees including background checks. Procedural security covers how cargo is handled in transit. It includes procedures designed to prevent, detect, or deter unauthorized people from gaining access to the cargo. Documentation processing involves recording and transmitting information about cargo.

Physical security is related to access control. The focus is on denying access to cargo by unauthorized personnel. This would include the use of fencing, parking, lighting, alarms, and video surveillance. Information and technology security covers basic information security such as passwords and IT security policies and practices. Security training and threat awareness reinforce the idea that security is everyone's responsibility, not just those assigned to security. The organization must create a program that informs employees of the need for security and trains them in identifying threats, such as suspicious activities, and that uses policies employees need to follow to increase security.

C-TPAT has five goals:

1. Ensure that C-TPAT partners improve the security of their supply chains pursuant to C-TPAT security criteria.
   a. Certify security profiles and security information provided by C-TPAT partners.
   b. Enhance validation selection approach using risk factors and expand the scope and volume of C-TPAT validations.
   c. Formalize the requirements for C-TPAT self-policing tool and implement the process for the submission of the C-TPAT periodic self-assessment.
   d. Require participants to engage and leverage all business partners within their supply chains.
2. Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners.
   a. Develop the C-TPAT secure communication platform.
   b. Conduct antiterrorism training seminars and targeted outreach for certified partners and the trade community.
   c. Share information and security best practices with the membership.
   d. Develop minimum security criteria, especially applicable to point of stuffing and smarter, more secure cargo containers.
   e. Provide expedited processing benefits to C-TPAT partners.
3. Internationalize the core principles of C-TPAT through cooperation and coordination with the international community.
   a. Partner with the international trade community to help secure global supply chains.
   b. Partner with individual customs administrations to improve the coordination of mutual antiterrorism efforts.

c. Support the work of the World Customs Organization (WCO) to develop a WCO-sponsored framework to secure and facilitate global trade that recognizes customs–private sector partnership.
d. Coordination with international organizations to improve the security and integrity requirements of their membership.

4. Support other CBP security and facilitation initiatives.

a. Support the implementation and expansion of the Free and Secure Trade (FAST) program.
b. Support the development and implementation of a more secure and smarter container.
c. Support and complement CBP's Container Security Initiative.
d. Support other CBP and Department of Homeland Security antiterrorism initiatives.

5. Improve administration of the C-TPAT program.

a. Implement the C-TPAT human capital plan.
b. Expand the structured training program for C-TPAT supply chain specialists.
c Coordinate with the CBP Modernization Office to enhance C-TPAT's data collection and information management capabilities.[1]

CONCLUSION

C-TPAT reflects the changing nature of supply chains. Organizations now have global supply chains. The security concerns for such far-reaching supply chains are complex. C-TPAT is one measure designed to have organizations think about and take action on their supply chain security.

See also Information Security; Integrating Physical and Information Security; Physical Security; Supply Chain Security; and Terrorism.

NOTE

[1] "Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan," November 2004, online at http://www.cfr.org/publication/11880/customstrade_partnership_against_terrorism_strategic_plan.html?breadcrumb=%2Fissue%2Fpublication_list%3Fid%3D135%26page%3D16 (accessed 14 March 2007).

GENERAL SAFETY CONCERNS

This section concentrates on a variety of mechanisms that share a concern for safety. These mechanisms include emergency preparedness, disaster recovery, business continuity, risk management, and crisis management. The focus is on how these mechanisms work to protect human and physical assets as well as how best to respond when these assets are threatened.

BENEFITS OF EMERGENCY MANAGEMENT

W. Timothy Coombs

If you are reading this book at work, do you know the quickest way to exit your facility? Most people are not familiar with the quickest exit route and would use the way they typically enter the building, which might not be the best option. How would you leave the building if your chosen route were blocked? Where would be your muster area? What should you do if an emergency requires employees to stay inside? These and many other critical questions can be answered through integrating emergency management into the workplace routine. Emergency management can be done as part of a business continuity plan, as part of a crisis management plan, or as a separate emergency plan. However it is done, organizations should be prepared for emergencies.

The attacks of 9/11 renewed interest in emergency management and preparation in organizations. Managers heard the stories of how better prepared organizations were able to evacuate their employees more efficiently after the attack than those that were unprepared. A terrorist incident is only one form of emergency. We usually think of emergencies as the purview of communities and government. However, organizations can have their own emergencies or be caught up in community emergencies. An emergency is any unplanned event (1) that can cause deaths or significant injuries to employees, customers, or the public; or (2) that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public reputation.

The term *disaster* is used to describe a large-scale emergency. All disasters are emergencies but not all emergencies are disasters. To avoid the subjective nature of the term *disaster*, the more general term *emergencies* is used in this entry. The process of preventing, preparing for, responding to, and recovering from an emergency is known as emergency management. Managers need to embrace the elements of emergency management and integrate them into their organizations.

Emergencies can be fires, severe weather, terror attacks, explosions, hazardous materials (chemical, biological, or nuclear), or natural catastrophes such as tornadoes or earthquakes. These emergencies pose a very serious threat to employees and others who happened to be at a facility, such as visitors or contractors. The goals of emergency management are to save lives, to prevent injuries, and to protect property and the environment—all extremely valuable goals for any organization. Emergency management is an investment in protection of employees and others who are on-site. Hurricane Katrina was yet another reminder that organizations in the private sector cannot be sure the government will take care of emergency management effectively. Organizations in the private sector, however, will bear the greatest casualties and costs of emergencies.

REVIEW OF THE EMERGENCY MANAGEMENT CYCLE

Emergency management revolves around hazards, which are events or circumstances that have the potential to evolve into an emergency. Hazards are closely related to risks. Refer to the entries Risk Management and Types of Risks for more information on the subject. An emergency management program identifies the hazards an organization faces, creates and enacts actions designed to reduce the hazards, works to prepare for hazards, and develops guidelines reacting to emergencies. Experts view emergency management as a four-phase process: (1) mitigation, (2) preparation, (3) response, and (4) recovery. This entry considers how each phase serves to benefit the organization.

Mitigation Benefits

Mitigation involves actions taken to eliminate or reduce a hazard and the risk it poses to an organization. It is similar to risk management. Mitigation is actually an ongoing process. People in an organization should be constantly evaluating hazards and searching for ways to reduce or eliminate them. Effective mitigation not only protects people and structures but also reduces the costs of response and recovery. The mitigation efforts are driven by the hazard analysis, which identifies what events can occur in or around a facility, the likelihood of those events, and the consequences of those events.

Some hazards can be eliminated, so prevention is part of mitigation. One example would be proper storm water management. Another form of mitigation is property protection measures, which serve to reduce the effects of a hazard on people and property. As with many other protective programs, employees have a role to play in mitigation. Employees should be educated about their role in reducing or eliminating hazards in an organization.[1]

Preparedness Benefits

Not every hazard can be mitigated. One example is an inability to control violent weather. Preparedness readies an organization for when a hazard does occur. The hallmarks of preparedness are plans and other preparations taken to save lives and improve response and recovery. The organization must develop an emergency management plan, assign and train employees to key roles, identify and stock necessary supplies, and assign areas for sheltering and muster points. The emergency management plan should be built around the needs to evacuate and to shelter-in-place. For each of these two central emergency management tasks, employees need to be assigned responsibilities for performing certain actions. Preassigning tasks increases an organization's preparedness. For instance, who will record employee names at the muster point or be responsible for sealing doors and windows with plastic? Make sure employees are trained in their emergency roles and can perform the necessary tasks.

The organization must be sure to have all the essential supplies. The basics include water, food, first aid supplies, and batteries. Other equipment is stocked as needed. The Shelter-in-Place entry provides more information about the materials required for that response. Crisis management plans and business continuity plans will include equipment lists as well. Coordinate the lists to avoid redundancy in stocking supplies. Finally, make sure there are designated areas for sheltering, mustering, emergency or other teams to meet; a storage area; and a distribution area for supplies. Predetermining the locations for these activities allows for a more effective response and less time wasted determining where things should go.

Employees should be encouraged to develop family preparedness plans and family emergency supplies. The Guidance Appendix provides outlines for family emergency planning and preparation kits based upon recommendations from the

Department of Homeland Security. During community-wide emergencies, employees need to know their families are safe. Plans can help to alleviate concerns along with allowing employees to contact their family members. Employees will leave to be with their family members if there are serious concerns about their safety. That is simply human nature.[2]

Response Benefits

When an emergency is about to hit or has hit, the response begins. Weather-related emergencies, for instance, often provide advanced warning. During a response the organization must provide assistance to victims and try to maintain continuity of critical systems. Refer to the Business Continuity entry for more information on maintaining critical systems. The organization's preparedness is put into action with the response. Decisions may have to be made quickly and be based on incomplete information. Exercises and drills allow your emergency team to hone decision-making and response skills. Refer to the Exercise and Training Basics entry for more detailed information.

Your organization may have to coordinate with governmental emergency management teams. This coordination is easier if an organization participates in community-based exercises and has a familiarity with the National Incident Management System (NIMS). NIMS outlines the structure of how an emergency response will unfold. Additional information about NIMS can be found in the NIMS box and in the Resource Appendix. Communities are required by law to

National Incident Management System (NIMS)

According to the Federal Emergency Management Agency, the National Incident Management System, or NIMS, "was developed so responders from different jurisdictions and disciplines can work together to better respond to natural disasters and emergencies, including acts of terrorism. NIMS benefits include a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid and resource management." NIMS is necessary because, even though most emergency situations are handled locally, there are times when state and federal responders must work together. NIMS is mandated by law. Private sector organizations are not required to be NIMS trained. However, having some personnel who are familiar with NIMS would make it easier for an organization to integrate its response with government agencies during a large-scale disaster. For more on NIMS, start here: http://www.fema.gov/pdf/emergency/nims/nims_doc_full.pdf.[3]

have regular emergency management exercises. Volunteer your organization to be involved in these drills. Your participation will increase your familiarity with the community response and improve your own emergency response skills.[4]

Recovery Benefits

The purpose of the recovery is to return the organization back to normal. This includes both facilities and activities. Clearly the business continuity efforts are instrumental in recovery, but recovery should also include learning. An organization must assess its emergency management efforts. What worked well? What worked poorly? What lessons can be applied to mitigation and preparation efforts? As with crisis and business continuity efforts, real events are a learning experience. However, we only learn if we review and reflect on our actions or inactions. Learning takes effort and is not automatic.[5]

CONCLUSION

Organizations should be concerned about emergency management and benefit from having effective emergency management programs. Emergency management is as basic as employees knowing how to evacuate a building during a fire or what to do when a tornado siren sounds. The increased threat of terrorism has made organizations revisit their emergency preparedness, and that is a positive step. Security personnel can play key roles in emergency management. They will be instrumental in efforts to evacuate or to shelter-in-place. Security personnel should be integrated into the emergency management teams. Moreover, emergency management efforts must look beyond terrorism to an all-hazards focus. The emergency management program is preparing for a variety of potential and likely hazards, not just one or two. An all-hazards approach is based on the fact that some elements of preparation and planning are relevant regardless of the type of hazard. The emergency management responses of evacuation or shelter-in-place can be adapted to any hazard. Management must make sure there is a broad, all-hazards approach to emergency management so that the organization is prepared for a variety of emergencies and benefits fully from an emergency management program.

See also Business Continuity; Community Emergency Response Team; Exercises and Training Basics; Risk Management; Shelter-in-Place; Emergency Response Training and Testing; and Types of Risk.

NOTES

1. Federal Emergency Management Agency (FEMA), *Principles of Emergency Management* (Washington DC: U.S. Government Documents Office, 2003), pp. 23.4–23.5.
2. FEMA, *Principles of Emergency Management*, pp. 3.9–3.15.

[3] "National Incident Management System," 1 March 2004, online at http://www.fema.gov/pdf/emergency/nims/nims_doc_full.pdf (accessed 8 May 2005).

[4] FEMA, *Principles of Emergency Management*, pp. 3.16–3.18.

[5] FEMA, *Principles of Emergency Management*, p. 3.20.

EMERGENCY PREPAREDNESS AND RESPONSE COMPONENT

Betty A. Kildow

In the continuing evolution of efforts to address the business challenges raised by disasters, we are becoming increasingly more capable and practiced in the areas of business continuity and disaster recovery. As this evolution continues, it is equally important not to forget the very foundation of a comprehensive approach to developing your organization's capability to respond to disasters—emergency preparedness and response.

DEFINING EMERGENCY PREPAREDNESS AND RESPONSE

As disaster-related terminology often varies from one geographic location to another, from one business sector to another, and between the public and private sectors, it seems reasonable to begin by establishing the definition of emergency preparedness and response used for this entry:

> *Emergency preparedness and response* has as its focus a plan of action to commence during or immediately after a disaster to prevent the loss of life and to minimize injury and property damage. It includes developing emergency response procedures and establishing training for all employees on the proper actions to take to respond to emergency and disaster situations and training for employee emergency response teams (emergency response teams, fire safety teams) on their roles and responsibilities. Also included is the acquisition and maintenance of life safety systems and emergency supplies and equipment.

EMPLOYEE PROTECTION AS THE PRIMARY GOAL

A comprehensive emergency preparedness and response program results in improved damage control and helps contain losses.

In every major disaster, one of the lessons that is reinforced is that although it is possible for an organization to lose its building, communications, and vital records and to pick up the pieces and move forward, it is impossible to continue or resume operations without the organization's most valuable asset, its employees. This was never truer than in the aftermath of the terrorist attacks on the World Trade Center in 2001. An emergency preparedness and response program's primary purpose and goal is the protection of every organization's most critical asset, its employees; and its secondary goal is the protection of its physical assets, such as its buildings and equipment.

All employees must understand your organization's emergency preparedness and response program and know and coordinate with those in charge of emergency preparedness and response planning. It is also a prerequisite for a comprehensive program that appropriate emergency supplies be in place, maintained in appropriate quantities, and well tested.

Most organizations approach meeting these goals first through the installation of life safety systems—such as security and alarm systems, smoke detectors, fire suppression systems, and access controls—and then through establishing emergency procedures to provide guidance for all employees for specific types of emergencies and disasters. Employee-staffed emergency response teams (ERTs) are recruited and trained and become internal first responders when an emergency or disaster occurs. Trained to fulfill their assigned duties, the usually volunteer ERT members provide initial assistance to protect the safety of employees and visitors until public safety agencies arrive. An emergency operations center may be established as a base of operations for those charged with managing emergencies, directing emergency response teams, assessing and controlling physical damage, coordinating with public safety officials, and providing status reports to management. This is an area in which the change in command and control between emergency preparedness and response and business continuity/disaster recovery must be predefined.

All employees should know the basics. To begin with, what does the alarm sound and look like? What is the correct way to make a 9-1-1-call? What am I to do when there is a fire in the building? An earthquake? A violent incident?

COMPONENTS OF AN EMERGENCY PREPAREDNESS RESPONSE PROGRAM

A comprehensive emergency preparedness and response program includes the following:

- Ongoing mitigation efforts to eliminate potential threats or lessen their impact
- Ensuring that life safety systems are sufficient for the physical plant and its population
- Organizing and training employee emergency response teams
- Developing, testing, and maintaining comprehensive emergency response plans
- Implementing awareness programs to make certain that all employees know

what the organization expects of them and what they may expect from the organization when disaster strikes
- Stocking emergency equipment and supplies that are inventoried and restocked on a regular basis (Rule of thumb: Be prepared to be self-sufficient for a minimum of seventy-two hours following a widespread or severe disaster situation.)

If you have cotenants in your building(s), work together to coordinate your emergency plans. Involve facility managers and property managers to be certain that procedures, evacuation routes, and the like do not conflict. Consider joint emergency planning.

In the past, the focus of emergency preparedness and response procedures and emergency response teams was to respond when someone was injured on the job or to get people safely out of a building in the event of a fire. Today that focus has expanded to include new threats to personal safety. The number of violent incidents in the workplace continues to grow, and there is an increasing frequency of hazardous materials incidents. The continuing threat of terrorist attacks and even a possible pandemic have now been added to this list of possible threats.

EMERGENCY RESPONSE TEAMS

Emergency response team members receive training on the overall emergency management program and their specific roles and responsibilities. Many organizations provide basic first aid, CPR, and blood-borne pathogens training, and possibly hepatitis B inoculations for team members. Basic evacuation techniques may also be included. In some cases ERT members may also receive training in the use of fire extinguishers. *A word of caution: The use of fire extinguishers by untrained persons can cause more harm than good.*

Some companies make first aid and CPR training available to all employees. This not only helps develop a workforce that is better prepared to handle emergencies while on the job, it also benefits the employees, their families, and the community.

An aging workforce has resulted in more employees with a cardiac history. As a result, installing an automated external defibrillator (AED) and providing the related training is increasingly common in the workplace. Initially used by public safety officials and now becoming increasingly common in public locations, an AED (defibrillator) is a computerized medical device. It can check an individual's heart rhythm, recognize a rhythm that requires a shock, and advise the rescuer when it is necessary to deliver an electric shock to a victim of sudden cardiac arrest to restore normal rhythm. AEDs are nearly unerring in properly assessing the need for defibrillation. If a decision is made to install an AED, it is crucial to provide ERT members with fundamental training (typically lasting approximately four hours) that includes basic use, as well as safety and maintenance.

CREATING AWARENESS AND PROVIDING TRAINING FOR ALL EMPLOYEES

Whereas trained ERTs are highly important, all employees must take ownership of their own safety and security and are responsible for following emergency response procedures. That being the case, it is vital that all employees receive regular training and refreshers on emergency procedures. Any plan and its procedures will be of limited value if all employees are not familiar with it or, even worse, do not know it exists. Be certain that all employees know what they are to do, their primary and alternate exit routes and assembly area, the members of their ERT, and what assistance will be provided to them when a disaster occurs. Making assumptions that people know what they are to do can lead to confusion and even panic when a disaster occurs, perhaps resulting in a loss of time that has devastating consequences.

Regularly scheduled evacuation drills in which *all* employees—no exceptions—participate are essential to making sure every employee, both ERT members and the general employee population, is prepared when the evacuation is not a drill but an actual emergency situation. Develop and implement a process to account for employees following an evacuation. Make certain that employees know where they are to go once outside the building and to whom they are to report. The purpose of the accounting procedure is twofold: first, to ensure that all occupants are safely out of the building and, second, to make certain public safety officials are not put in harm's way while looking for people who are no longer in the building. Work with local public safety officials to be certain your assigned assembly areas are appropriate for that purpose and will be safe gathering places out of the way of emergency equipment.

In today's multicultural environment, don't forget that those whose first language is other than English may also be using your emergency procedures and signage, evacuation instructions, and so on. Depending on the building's inhabitants, signage in multiple languages may be necessary.

ESTABLISHING AND MAINTAINING AN EMERGENCY COMMUNICATIONS SYSTEM

Have a means of notifying employees that a disaster has occurred off-hours. This can be done through any of a wide choice of methods from the old standby "telephone tree" to the new, sophisticated notification systems. Let all employees know the type of event, its initial impact on the organization and its facilities, and, if known, when they may expect to return to work. Then, keep them aware of progress with periodic updates. Establishing an out-of-area 800 number that employees can call to hear status updates following a disaster or serious emergency is a cost-effective way to provide them with vital information. Remember, an information void leaves room for incorrect information to be inserted.

MAINTAINING EMERGENCY EQUIPMENT AND SUPPLIES

Each organization needs to maintain and regularly inventory recommended first aid supplies. Your local office of emergency services and Red Cross are good sources for a list of recommended items. Evacuation devices, water purification tablets, plastic sheeting, dust masks, gloves, light sticks, and sanitation supplies are some of the things that may be among an extended cache of supplies and equipment. Whether to maintain a three-day supply of water and food for each employee is a policy decision and may be based on regulations or on how likely it is that a disaster would require employees to stay at the work location for as long as three days.

Surprisingly, you may find that there is already a sufficient supply of water and other beverages in your building in the cafeteria, kitchens and break rooms, water coolers, and vending machines.

Once stocked, emergency supplies must be properly maintained. In particular, some first aid supplies and emergency food and water have a shelf life. Inventory all equipment and supplies not less than annually, discard and replace dated items, and replenish supplies as necessary.

EMPLOYEE SPECIAL NEEDS AND SKILLS

In the United States, the Americans with Disabilities Act (ADA) is a federal civil rights law that prohibits the exclusion of people with disabilities from everyday activities and includes a requirement that the safety and evacuation special needs of all employees are met. If employers covered by the ADA have emergency evacuation plans, they must include people with disabilities. Beyond meeting regulatory requirements, meeting special evacuation needs of those with disabilities is morally and ethically right. Emergency procedures should include special provisions to provide the assistance needed by all employees with special needs, such as the mobility impaired, visually impaired, and hearing impaired. For example, employers may need to have emergency evacuation devices and plans for employees with disabilities as a reasonable accommodation.

In some cases, the need for additional assistance may not be obvious, or as the result of an accident an employee may temporarily require special assistance. To help identify those with special requirements, an employee special needs form may be distributed with an invitation to employees to complete and return the form. The key word here is *invitation*. Completing and submitting the form must not be mandatory. A periodic reminder to all employees of the importance of maintaining a three-day supply of prescription drugs and other medical supplies and devices at work is a simple, yet important, step in helping ensure that all employees are prepared in the event of a serious emergency or disaster that may require them to stay in the building for an extended period.

To aid in staffing emergency response teams and to identify employees who may be able to assist following a disaster, organizations may opt to survey employees. There are often "hidden assets," employees who possess skills or knowledge that may make them particularly qualified as emergency response team members or provide much-needed help in a disaster situation.

ARE YOU READY FOR AN EMERGENCY?

Responding to the following twenty-five questions will provide a basic assessment of your organization's emergency preparedness and response program. Simply answer each question with a yes or no. There is no partial credit, and not knowing an answer equates to a negative response.

Give yourself five points for each yes; zero points for each no. How did you do? Although this assessment is not extensive, it provides a good indication of how well your company is doing to prepare to face the next disaster.

1. Is your building equipped with life safety systems, such as emergency lighting, fire suppression system, a fire alarm system, and fire extinguishers?
2. Do you have an up-to-date emergency preparedness and response plan, one that has been reviewed and updated within the past six months?
3. Does your organization provide each employee with a printed copy of its emergency procedures and post the procedures in all public areas of the building(s), such as reception area, conference rooms, and break rooms?
4. Have you conducted a threat assessment analysis to determine the hazards and threats (natural disasters, technological disasters, human-caused disasters) that may impact your organization?
5. Have you instituted a comprehensive mitigation plan to eliminate or lessen the impact of identified threats?
6. Do you have an evacuation plan? If so, do you review and, as necessary, update this plan not less than annually?
7. Are all employees within your organization familiar with your emergency response plan, and do they know what to do for each type of emergency situation?
8. Does your organization provide new employee orientation to emergency procedures and not less than annual emergency

(continued)

response refresher training (evacuation, bomb threats, medical emergencies) for all employees?

9. In the event of an evacuation, have you determined shutdown procedures to be followed, guidelines for when to follow/not follow the procedures, and designated employees to do so?
10. Do you have employees in each location who have current certification to provide first aid and CPR?
11. Have you designated and trained employee emergency response teams (ERTs) to respond to emergency situations?
12. Do your employees know locations near your building(s) where emergency medical care will be provided after disasters?
13. Have criteria for evacuation and sheltering-in-place been established?
14. Do all employees know how they will be notified if it is necessary to evacuate or shelter-in-place?
15. Is there a system for accounting for employees following an evacuation that includes having assembly areas outside the building?
16. Does the company maintain daily records of visitors, in addition to staff, in the building?
17. Have you conducted a full-scale drill of your evacuation plan within the past six months?
18. Have you set up procedures and lines of communication to provide information to employees after a disaster occurs?
19. Have you established a damage assessment process and identified who will conduct the assessment once public safety officials declare it is safe to reenter the building?
20. Do you have a program in place to help employees address the emotional response to a disaster that impacts your organization and/or its employees?
21. Does your organization have an enforced policy that all visitors to your building(s) be escorted at all times?
22. Do you have a process that ensures that in an emergency or an evacuation drill special assistance will be provided to employees and visitors who have mobility, sight, hearing, or other special needs and have indicated that they require assistance?
23. Have employees been trained to recognize suspicious mail and packages, and do they know what steps to take if one is received?
24. Does your organization encourage employees to prepare their homes and families for disasters?
25. Can you personally name the members of the emergency response team for your area at work?

125 points	Congratulations to you and your organization—keep up the good work.
100–120 points	Very good. Take another look at the questions to which you responded "no" for areas for enhancement to make your emergency preparedness and response program even better.
55–95 points	Although your organization has made an effort to prepare for disasters, there's room for substantial improvement. Develop a plan to lessen the gap between where you are and where you need to be.
0–50 points	A great deal of work needs to be done—quickly. Get the right people involved, consider getting some outside help, and get started.

PERSONAL PREPAREDNESS

It is also important to remember that disasters that strike the organization often also impact people's homes and families. During and following a widespread emergency or disaster, employees often find themselves torn between competing demands. While most are dedicated to the business and to their responsibilities to the organization, they are also committed to their homes, families, and communities. These competing roles create challenges during normal times, and when a disaster impacts both home and work the challenges are multiplied many times. This role conflict creates a situation in which employees can find themselves torn between competing demands on them to fulfill work roles versus their roles as family members or protectors of loved ones. In turn, this conflict may cause guilt whether the employee is at home or at work.

Businesses and organizations can help alleviate this role conflict by providing encouragement and assistance to employees in preparing their homes and families to face disasters. Implement a plan to assist employees in making their homes and families disaster ready by providing training. This can start with providing printed informational material on disaster preparedness for the home to all employees. Offering disaster preparedness training and workshops is a further step. Also consider holding an annual "disaster fair" so that employees can purchase emergency supplies and equipment from suppliers who display their products at the work site. If possible, deduct the cost of employees' purchases over several pay periods. Helping prepare employees for disasters at work and at home is a win-win-win. It benefits employees, the organization, and the greater community.

And as we think about home emergency preparedness, let's not forget to look inward. Some of us involved in emergency planning may be like the shoemaker's children who have no shoes. We let slide making our own emergency preparations, neglecting to prepare our homes, our families, and ourselves to face the next disaster. This lack of preparedness can prevent us from being available and able to give our time and attention when we are needed to play our assigned role in our organization's emergency response, business continuity, or disaster recovery plan. Check. Do you maintain emergency supplies and equipment that include water, food, first aid supplies, clothing, bedding, basic tools, and items for those with special needs (e.g., infants, elderly, those with medical needs)? Do all members of the household know what do when disaster strikes? Do you have a home evacuation plan, and do all household members practice following the plan not less than twice a year? Have you established an out-of-area emergency contact telephone number, and do all household members know about it and keep the number with them at all times? Have you developed a list of emergency numbers that is easily accessible to everyone with a copy near each phone in the house? If there are children in the home, are you familiar with the school's hold/release emergency plan? Does everyone in the home know how to call 9-1-1? Prepare yourself and also educate all employees on the importance of being prepared at home.

CONCLUSION

Preparedness is the key to protecting the business and its people. Companies with an effective emergency preparedness and response program in place are prepared to protect their employees, visitors, and properties. As the evolution of emergency management continues, it is essential to develop and maintain robust emergency preparedness and response programs. These programs will help avoid your organization's being viewed as being ill-prepared when, not if, the next major emergency or disaster occurs.

See also Benefits of Emergency Management; Exercise and Training Basics; Emergency Response Training and Testing: Filling the Gap; and Evacuation in Large and Multiple Tenant Buildings.

COMMUNITY EMERGENCY RESPONSE TEAM

W. Timothy Coombs

The Community Emergency Response Team (CERT) is a program that educates people about emergency preparedness. Community members are trained for hazards that are likely to affect their areas and in basic emergency response skills. These skills can include first aid, search and rescue, and fire safety. Although the focus is on helping the community, CERT also recognizes that its training can be beneficial in the workplace. CERT members supplement professional responders and step in when responders are not immediately available. CERT members should also take an active role in community emergency preparedness projects.

To become a CERT member, a person has to complete emergency management training that local governments offer. CERT is part of a larger effort by the Department of Homeland Security to get people involved in preparedness and security through Citizen Corps. Citizen Corps encourages people to take personal responsibility for preparedness by getting trained in first aid and emergency skills and to volunteer to support local emergency management. Organizational management should consider encouraging some employees to join CERT. Those involved in the emergency management team, including security personnel, would be likely candidates. Employees who are involved in CERT have a better understanding of the threats in their community and have training in how to lessen the effects of those threats. CERT employees can be a valuable resource for an organization.

See also Benefits of Emergency Management; Disaster Recovery Management; and Emergency Preparedness and Response Component.

EMERGENCY RESPONSE TRAINING AND TESTING: FILLING THE GAP

Ágnes Huff

Much of the effort for crisis management and disaster response has been focused on planning and documentation, which is undoubtedly an excellent starting point. This initial part of the planning process tends to occupy the bulk of the effort and the major share of the budget. Once a plan is completed, or well underway, the organizational tendency is to move on to other pressing business priorities. This leads to a false sense of security that “we have a plan,” so we are prepared.

The process of planning is extremely valuable and positions an organization as proactive and competitive. Whether it’s loss of momentum near the end of projects, lack of resources, or personnel or leadership changes, the process is assumed to be finished. When most of the initial effort is allocated to development and much less is devoted to training and testing, the gap leaves an organization vulnerable.

Crisis response becomes a priority when something dramatic or devastating happens within the organization, in the community, or in the industry. Following a crisis, a small window of opportunity exists to revisit preparation before the corporate equilibrium returns to previously inadequate but comfortable levels.

Proper training and validation ensure that responders understand their roles and responsibilities; are aware of available resources and communication protocols; comprehend organizational goals, objectives, and rationale for crisis procedures; and are cognizant of how everything fits into the overall response scheme.

Often, plan testing is done infrequently or sporadically, especially in cases in which it is not mandated by regulatory agencies. Sometimes a rush to test the plan prematurely without providing the necessary training to personnel creates a "learn by failure" environment and is detrimental to the program.

INVESTING IN TRAINING

Training and testing of crisis management plans teach proper response actions, rather than leave people to depend on their usual reactions. Training facilitates coordinated response and team building, which are essential goals for effective response. It also develops self-confidence on a personal level, increases efficiency on the professional level, and speeds and maximizes response. An organization's reputation and future business success can depend on its investment in training. The training phase comes first; then comes the testing phase.

Adequate training allows for an examination of a wide range of crisis situations with opportunities for intellectual rehearsal. This provides a framework for proper actions in similar situations and fosters the team creativity required for optimal response.

A well-developed training program needs to stress flexibility in managing crises, including revising the situation analysis as a crisis unfolds. SWOT analysis (strengths, weaknesses, opportunities, and threats) provides insight that helps to refine response options. It teaches crisis team members how to identify and prioritize business activities.

Crisis training should be done for specific crisis families—natural disasters, technological crises, business crises, and those caused by humans (workplace violence, etc.)—because it is not realistic to try to plan for every eventuality. These broad crisis categories expand the team's knowledge base by identifying similarities within crisis families.

A detailed action plan that identifies key learning to be incorporated into the plan should follow every training session. This ensures that the plan development, training, and testing process maintains relevance and validates its effectiveness in a crisis.

Training should begin on the local/division level and then get increasingly more comprehensive throughout the organization and even include external partners or resources. An effective response plan ensures that each division and department has internal processes that fit in with the overall corporate plan.

Unless an organization is in a high-profile, high-risk regulated industry such as shipping or transportation, senior management commitment is required to ensure that daily business priorities don't supersede crisis management training and testing.

THE HUMAN ELEMENT

Crisis plans are not replacements for well-trained responders. Plans are dependent on the most variable element, the human element. This interdependency between people and plans is what necessitates focus on this important issue for training. The ways people respond—their coping skills, emotional state, leadership expertise, decision-making capacity, resourcefulness, ability to work under pressure, cooperation in a team environment, and how resourceful they are—are part of their human personality. Individual characteristics and attitudes, as well as human frailties, impact abilities in responding to crisis. Inadequate preparation, briefing, or training puts a disproportionate burden on the individual, rather than on the system and process of response.

Plans are only a guide to help people focus on the key activities and procedures that are frequently experienced in highly dynamic and overwhelmingly stressful crisis situations. It takes well-trained people to understand, appreciate, and execute the plan to the best of their collective abilities in a disaster or crisis situation, which further supports that training is one of the most critical activities that can determine whether response is effective. Furthermore, strategies to manage the human toll that disaster responders experience should also be included in the training, such as coping strategies for stress management, defusing, and critical incident stress debriefings as the situation or crisis warrants.

For prepared and progressive organizations, familiarization, response, and special skills training courses are mandated for team members initially and on a regular refresher schedule, and definitely should never be left to chance.

TESTING IS VALIDATION

Many plan testing methods exist, and organizations need to allocate personnel and financial resources to conduct a periodic validation and verification that the response plan, as developed, can and does function appropriately. One of the main areas that requires regular testing is the notification system that tests the organization's ability to mobilize responders. Without the capability to contact and mobilize key responders in the aftermath of a crisis, an organization may face unnecessary delays in the vital crisis response.

Notification and a call down test can be conducted within internal departments as well as with outside resources relatively easily. No plan can be optimally effective if it doesn't provide a mechanism for bringing the right people together quickly to initiate the response. Verifying through regular testing that it is a "fail-safe" contact system is by far one of the most fundamental and valuable activities, yet it is often overlooked.

Testing allows every aspect of response to be audited, reviewed, and evaluated to identify shortcomings, serious problems, and potentially overlooked issues in advance of a crisis. A simple follow-up audit and recommendation report highlights key learning and identifies needed actions. The final step in the validation process is approval and incorporation of the revised procedures, followed by subsequent future testing to bring the process full circle.

From notification tests, tabletop drills, role playing and full-scale simulations involving outside entities, to the latest interactive methods with online technology, all organizations must plan, conduct, and evaluate the results of their validation exercises. Testing whether the plan works under simulated real-world conditions achieves one of the major objectives.

SCENARIOS

The most effective exercise scenarios are those that are based in reality for the organization. When participants feel they can identify with a crisis situation, they are more likely to be engaged in the overall process. Scenarios can be simple or extremely complex. The goal is to have manageable scenarios that can introduce relevant and challenging facts that stimulate and test participant problem solving, their resourcefulness, and teamwork in the process.

Rigorous standards should be applied during any test or simulation to eliminate the human tendency to potentially characterize outcomes more favorably than they really are. For maximum effectiveness, scenarios should be planned for each of the four crisis categories so testing maintains relevance, variety, and maximum benefit over time.

ROLE PLAYING

Role playing is an excellent training and testing tool that is frequently employed by law enforcement agencies, educational institutions, and counseling programs. Providing opportunities to interact in a simulated real-world crisis situation provides a uniquely beneficial training experience, especially for training in human interaction, communication, and leadership skills. As communication principles underlie nearly every aspect of effective crisis response, the incorporation of role playing into the overall training program provides the chance for responders to demonstrate essential skills.

Building skill requires practice and repetition. In addition to developing expertise, role playing fosters team building, creative thinking, and understanding of others' roles and responsibilities through a relevant teaching tool.

TABLETOP EXERCISES

Tabletop exercises, also known as table-talk exercises, can be used both for initial response training as well as for plan testing. Participating in a planned half-day exercise allows people to experience "working through" a relevant crisis scenario and to develop response strategies collectively. Discussion of different perspectives, assumptions, and needs is combined with the opportunity to evaluate the consequences of actions through the exercise. Receiving feedback and engaging in a dialogue with others provides valuable insight not otherwise available.

Tabletops can begin as a group and then break into smaller team sessions to identify what must be done and how. Following the breakout meetings, the group gathers to discuss the entire scenario and how each team is integrated into the response. Tabletops facilitate an understanding of weaknesses and the need for additional resources. Along with the other training and testing methodologies, tabletops can be incorporated into crisis plans as effective training tools.

SIMULATIONS

Simulations have been used for many years for training and testing in aviation, in the military, and increasingly in the medical environment. They draw on cooperative group experience with realistic events, utilizing the range of tools available for managing a crisis. Crisis simulations are able to test crisis management capabilities in highly stressful situations. Benefits include insight into organizational behavior, individual functioning, group interaction, communication, and leadership, resulting in greater overall response coordination.

Extensive planning and preparation are required to conduct useful simulations, including individuals to serve as facilitators and objective observers for the ultimate evaluation of the exercise. Simulation training identifies strengths, vulnerabilities, and responses under stressful conditions for the critical goal of improving capabilities and fostering self-confidence in the response.

INNOVATIVE PRACTICES: VIRTUAL REALITY

Testing an individual's judgment, decision making, and communication with others provides an integrated approach and allows for appropriate feedback and guidance to enhance performance. Innovative companies are developing virtual reality (VR) simulations, which can provide more realism in a safe training environment. VR allows for repetitive opportunities to try different actions and experience their consequences in an interactive, dynamic, and engaging format that is impossible in the real world. Greg Hendricks, retired commander of the Portland, Oregon, Police Department, summed it up well when he said, " . . . exercises and field exercises test plans. Gaming and simulation test people."[1]

The Advanced Disaster Management Simulator (ADMS™) has the capability to provide team training on the incident command system employed by emergency services agencies. It can simulate aircraft accidents, terrorist acts, hazardous material spills, natural disasters, and disasters as a tool to improve overall crisis incident response.

Another VR incident management project by Marintek, the DISCOVER project, is developing two real-time training and assessment simulations for the petroleum and maritime sectors with the goal of more effective training for improved safety in these high-risk industries.

As technology advances, VR training will be able to provide more accessible and cost-effective alternatives with enhanced increased flexibility and greater psychological realism.

CONCLUSION

Training and testing are directly linked and form two of the most critical elements of the crisis response and business continuity process. Like all business processes, crisis plans must be top of mind and validated regularly to ensure their effectiveness. With crisis planning, training, and testing, an organization maximizes its ability to protect lives, property, and its assets, as well as to safeguard its reputation and business.

See also Benefits of Emergency Management; Business Continuity; Crisis Management; Evacuation in Large and Multiple Tenant Buildings; and Exercise and Training Basics.

NOTE

[1] Greg Hendricks, “The Imperative,” online at http://www.crisissimulations.com/risk_reality/imperative.html (accessed 25 March 2007).

DISASTER RECOVERY MANAGEMENT

Robert C. Chandler

> *Emergency response is a product of preparedness. On the morning of September 11, 2001, the last best hope for the community of people working in or visiting the World Trade Center rested not with national policymakers but with private firms and local public servants, especially the first responders: fire, police, emergency medical service, and building safety professionals.*[1]

Recent history suggests that disruptive disastrous events, even at some distance from a company’s facility, may disturb routine operations or put personnel and business at risk. Business continuity planners must therefore anticipate and prepare for the potentially significant disruption due to a disaster. Whether it arrives via a category 4 hurricane, a major earthquake, an armed intruder, an act of terrorism, an industrial accident, a train derailment of toxic chemical, or a fire in a data center that results in the loss of mission critical information: preparedness and planning for disasters and recovery of operations is a due diligence obligation for every business and organization no matter the industry, field, or location.

The process of preparing for catastrophically disruptive events may be termed *disaster recovery*, *contingency planning*, *business continuity*, *business resumption planning*, *contingency management*, or *crisis management*. No matter the label, it remains a vital and important series of tasks on which great stakes hang in the balance, including financial, continuity, reputation, and the health, safety, and even life/death of people. Planners face the challenge that many of the different types of threat risks and possible categories of disasters require unique response plans to mitigate and start recovery. An organization must develop plans that review areas of vulnerability when improvisation is impossible, even for the most experienced businessperson.

Several areas to consider are preparedness planning, mitigation activities, and recovery planning. One step of preparedness planning is the assessment of your hazard vulnerability. What hazards can cause the most damage to your facility and operations? What sort of damages? Can you lessen the impacts of those hazards? Mitigation activities include reducing both structural and nonstructural hazards through reinforcing buildings, anchoring light fixtures in ceilings, bolting bookcases to wall studs, and protecting computer equipment. Recovery planning involves making provisions for first aid, search and rescue, building evacuation, and emergency communications; coping with fires and hazardous materials; and general personnel training in all of the above. Even the best of disaster management planning may not be sufficient unless senior management has bought in to the plan and made a serious commitment to this process. The most successful plans promote a constant awareness among employees, who, in turn, influence senior management to put a plan in place. Commitment without resources (money), however, is not a real commitment. Diligent companies must take heed of these threats, assign the necessary resources, and prepare accordingly.

MAJOR CATEGORIES OF DISASTER THREATS

The breadth of an effective disaster recovery plan is significant in the post–9/11, post–Katrina, post–Virginia Tech world. Enterprise-wide disaster preparedness planning is important for all mission critical operations against all categories of threats. Disasters may be localized, regional, or even nationwide. For the most part, focus on how the disaster (no matter how widespread or pervasive) affects your operations and your people. Although no list can be considered exhaustive, disasters can be organized and categorized into a number of general categories, such as according to their source (cause) or their impact.

There are at least five ways to categorize disasters based on the source or cause:

1. *Natural disasters* arise from environmental and weather-related elements that threaten business operations, health and safety, and business continuity. These include the threats from hurricanes, tornadoes, wind, winter storms (i.e., ice hazards, heavy snowfall, blizzards, extreme cold, etc.), earthquakes, landslides, floods, pandemics, and wildfires.
2. *Industrial accidents/mechanical failures disasters* include those that arise from equipment, facilities, transportation, and product or chemical containment failures. These threats may come as internal aspects of your operations or from external sources (e.g., a nearby train derailment). Typically, accidents result in disruptions and threats from spills/leaks, containment breakdowns, mechanical failures, product defects, and utilities interruptions.
3. *Malevolent act disasters* include those that occur due to the deliberate (intentional) actions to create damage, harm, injury, and disruptions regardless of their motive or rationale for such actions. These threats may arise from intruders or from current or former employees. Typically, they take the form of kidnapping, hostage taking, workplace violence/homicide, criminal actions, vandalism, and acts of terrorism.
4. *Data or information loss disasters* include those that arise from direct or indirect disruptions to information technology systems, data processing, records, communication, and Internet or web-based applications. Direct threats include computer hacking, denial of service attacks, disgruntled employee vandalism, financial or identify theft, and corporate espionage. Indirect threats happen when a primary disaster (e.g., flood, fire, storm, etc.) results in a loss of data, destruction of information technology equipment and/or facilities, or limited access to mission critical data or information technology functions.
5. *Human error disasters* arise when the mistakes or poor decisions of key people result in a catastrophic disaster in a variety of different ways.

There are also at least five ways to categorize disasters based on the impact to your business:

1. *Facilities/equipment* can be destroyed outright or simply become inaccessible due to a disaster. Key considerations for any loss of facilities and equipment are alternative work sites, telecommuting, backup locations and equipment, communication (including notification and rich media alternatives), and a plan for resumption of operations. Each type of disaster poses unique threats to your facilities and equipment.
2. *Personnel* (e.g., health, safety, and well-being impacts) can be put at risk during disasters. Questions about training, resources, supplies, preparedness, evacuation, shelter-in-place, emergency care (medical and psychological),

and various needs of your people need to be addressed. Each type of disaster presents unique threats to your people and personnel.

3. *Data/IT* impacts include the loss of mission critical data or systems, the loss of functionality, and the time it takes to be back up and running.
4. *Production operations/systems* include all of the various processes, procedures, and daily activities (including sales, marketing, production, delivery, etc.). Each type of disaster poses unique threats to your operations and processes.
5. *Reputation or corporate image/brand* disasters are one of the most recent "crisis management" impact topics for disaster management and recovery. Because the reputation or brand of your business has a value, anything that damages that value can be considered disastrous. In fact, a major ethical misconduct disaster can overwhelm and destroy even the largest corporation (e.g., Enron). A serious corporate scandal or malfeasance can quickly snowball into a full-fledged disaster that disrupts operations, demoralizes the workforce, deters investors and customers, and perhaps leads to the extinction of the business itself. When considering all the above, it is important to think about the abso\lute worst-case scenario as well as the most likely risks in a threat analysis.

DISASTER RECOVERY MANAGEMENT

Disaster recovery management involves not only planning but also conducting regular exercises and simulated emergency situations. These keep personnel up to speed on their emergency response and recovery roles. Furthermore, past experiences in disasters suggest that it is prudent to encourage employees to develop their own emergency plans at home, because people who are confident about the postdisaster well-being of their families will perform better at their workplaces.

As you review recovery planning, determine which elements of your operations are the most important for continuity of business, how to protect or restore those elements, and who can help you after a disaster if your own resources are overtaxed. It is also crucial to develop methods of communicating with your suppliers and customers.

RISK ASSESSMENT

All organizations must assess which types of disasters potentially threaten them, where they are the most vulnerable, the cost of preparedness versus risk probability, and the costs of being unprepared, as well as how they can allocate the time, energy, and resources to best prepare. Prioritize your assets and protect them accordingly.

Ultimately, of most importance is the survival of your company and the attempt to minimize losses of the owners and shareholders. Although it is obviously very important to protect both your people and your customers, do not forget about the shareholders who also rely on your company's prosperity.

To begin this process, review all of your business operations thoroughly, paying particular attention to the people, processes, and equipment/data/facilities critical to your mission and continuity of operations. Center disaster recovery management on your particular business needs, and answer questions such has how long a "downtime" your business could survive without key personnel, data, systems, faculties, delivery, or sales access. A thorough and comprehensive review of business functions (considering the details, not just the big picture) is important. It may be necessary to lay out flowcharts, process diagrams, or other means to "get a handle" on how the interconnection of all aspects of your business are coupled (or decoupled) to other aspects in order to understand the impact of one aspect's disruption or loss on the overall system.

Disaster recovery management is much more than merely arranging for backup options (although having a plan B is certainly a key aspect). This process seeks to balance risk management and insurance aspects, prevention steps, mitigation and protection procedures, a focus on personnel, continuous availability of mission critical processes, as well as the short- and long-term continuity of the business operations. In addition, the disaster management process should incorporate input regarding legal and regulatory compliance; contractual stipulations concerning continuity, availability, and disaster management; public relations and organizational reputation; human resources and/or labor concerns; and privacy and confidentiality issues. Planning should also take into account providing essential safeguards and protections for employees as well as members of the nearby communities.

Once you have a good "snapshot" of your business processes, begin considering, systematically, how various disasters might disrupt these processes and what such disruptions would cost your business. This procedure is often called a business impact analysis (BIA).

CONDUCTING A BUSINESS IMPACT ANALYSIS (BIA)

One of a planner's first priorities is to systematically analyze the potential harm, disruption, and costs of various disasters for the organization and its specific industry, locations, and exposure. The goal is a precise forecast of the threat risks of each disaster. However, it is challenging to predict accurately some of the risks of local, regional, and national disasters, such as terrorism attacks. Further, because of the wide variety of potential forms of disasters, it may be helpful to seek external resources—such as security services, insurers, disaster recovery professionals or associations, consultants, or law enforcement or government agencies—to assist in reviewing the company's unique situation. Resources are available from both private and public sector agencies to assist in this process (see the Resource Appendix for a partial list of these resources).

The BIA should examine each potential impact and identify its direct and indirect results. Usually these types of impacts can be quantified in terms of productivity losses or in financial terms, but do not overlook the intangible losses that are more difficult to quantify but no less important to your business. Typically, senior management expects you to provide some quantification to your BIA in order to determine "acceptable" versus "unacceptable" loss threats. This is also a good opportunity to tie the BIA process to the core values or key mission of your company or organization. Draft a summary of the types of exposure risks, and assess (quantifying risks, if possible) the potential costs of such disasters. Once you have a clear idea of what is at stake in terms of potential disasters, move on to the questions of limiting the loss risks and minimizing the potential impact of these disasters to your business operations.

In conducting a BIA, take the process of scanning for risks out of the sensational frame and into more specific logical and well-thought analysis. Some companies that have long used risk models for natural disaster risk analysis, for example, have begun to adapt those resources to create probabilistic models for various disaster risks. One resource to consider is your insurance provider.

The general process of assessing threats begins with a single focal point within the organization (either a specific type of disaster or an impact of disasters). Then discuss thoroughly the implications of the disruptions that a disaster creates. Subsequently, expand, in a systematic fashion, the parameters of the analysis to all aspects of your operations for a given disaster. How would every type of disaster impact a given operation? Consider all potential vulnerabilities.

Develop a method to assess threats and what actions can mitigate the damage. It is difficult to predict how, when, or where a disaster will strike; therefore, everyone must be prepared. Have a crisis plan for all categories of disaster events so you can institute responsive control measures rapidly when disasters occur. Consider, too, how to protect personnel during all types of disasters. Implementation of planning for disaster management as well as postdisaster recovery work require close collaboration among the company and local law enforcement, emergency responders, public health agencies, and government officials.

In sum, the BIA's usable "bottom-line" report of thorough analysis should clearly do the following: (1) articulate the key areas at risk for each disaster scenario, (2) provide an analysis of the loss (cost) potentials for each, (3) quantify these impacts in appropriate terms for your company, (4) identify mission critical vital functions/applications and acceptable disruptions, (5) determine emergency alternative (backup) operating methods for each and the costs required to have these available, and (6) establish minimum resources necessary for assurance of continuity of operations with the recovery resources available.

PROTECTING ASSETS, OBLIGATIONS, AND OPERATIONS

Establish the disaster recovery management's mission within the larger context of your organization's business goals and objectives. This helps determine which assets, obligations (explicit contractual or implied/assumed), and operations are priorities for protection or recovery. In many cases, specific service-level agreements (i.e., availability articulations, minimally acceptable downtime, etc.) can be useful in making choices about what to protect or to prioritize for resumption of service efforts. If you have not already done so, establishing the service-level expectations during various disaster scenarios or situations helps in determining your priorities for protecting or recovering specific assets or operational capacity. In any event, have a road map that gives everyone a consistent plan to follow for protection priorities, recovery targets, and timetables. These priorities should be articulated and well understood by everyone (top to bottom) so that there is a clear sense of "what comes first and what comes next" during and after a major disaster. Obviously, recovery sequence priorities will differ depending on your business, location, or mission. Furthermore, such priorities may or may not mirror your routine business priorities due to decisions about deployment of recovery resources, the time required to fully implement recovery, or your company's "bright line" decision that lives and safety come first regardless of cost or impact. In general, assets are protected to ensure availability for mission critical functions and to mitigate hazards and threats to personnel.

At this step in the planning process, consider possible alternate facilities or equipment, crisis communication plans, personnel protection (e.g., evacuation plans, shelter-in-place, etc.), data and information security, human resources policies (e.g., bereavement, sick leave, etc.), emergency response, life safety protection (e.g., medicines, food, water, shelter, etc.), and alternative work arrangements.

Disaster recovery's role in protecting assets and operations casts a wide net. The topics covered include data processing/IT disaster recovery and protecting personnel.

Data Processing/IT Disaster Recovery

Once you have determined the mission critical aspects of your data processing and information technology (IT) operations, as well as set the minimally acceptable downtime for these functions, plan to mitigate any potential disaster impact. A thorough BIA analysis as it relates to data processing and IT operations would include consideration of reciprocal agreements, continuous availability options, whether or not the building can be occupied or when occupation of the building can occur, and a status review of all your assigned data processing and IT operations personnel. The latter should include a look at data processing and IT operations shift rosters; the status of data and record storage both on-site and off-site; vital records policies; appropriate remote sites; mirror-site data processing alternatives;

contracts for data processing or alternate site operations; emergency maintenance for all equipment and support systems; and commercially available recovery facilities, services, and vendors.

Protecting Personnel

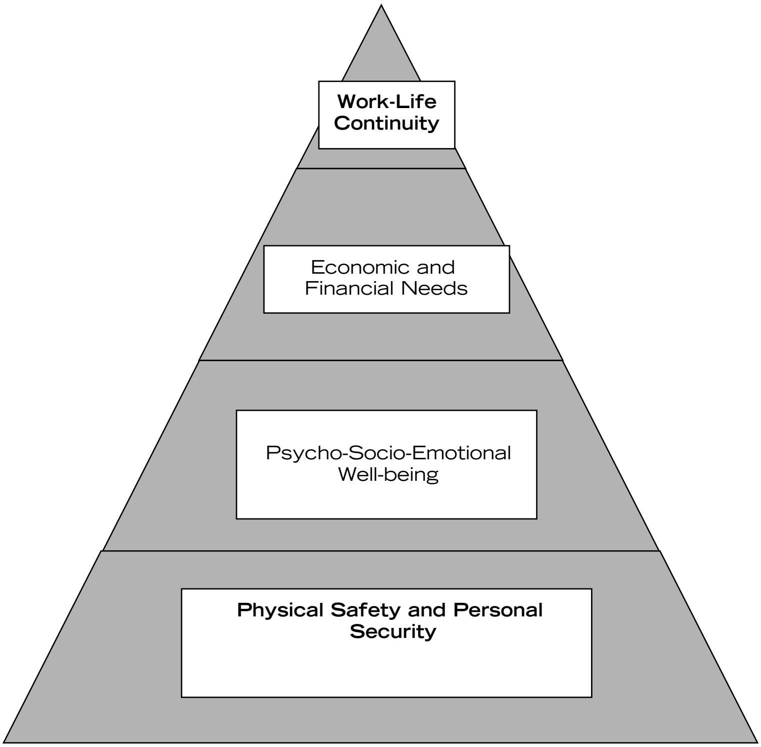
It is important for a business to protect its assets. A large part of risk management involves insurance, reinsurance, and reducing potential financial liabilities. However, given the variety of potential disasters and impacts, one asset that deserves substantial consideration for protection plans is your workforce. Obviously, protecting people is a moral and ethical imperative. No other material possession is worth more than the people whose lives are, in part, entrusted to your protection. No cost-benefit analysis could ever replace the fundamental obligation of prudent organizations to protect the people within and near their locales.

Protecting people is also a legal requirement. Those in management or ownership positions have an implied contractual and due diligence obligation to guard the health and safety of others in the workplace. Further, various governing agencies and regulatory bodies enforce numerous requirements to ensure their protection. However, your personnel are actually one of your greatest assets. No capital reserve, bond, equipment, or property is worth more to your company. If you account for the intellectual capital, institutional creativity and memory, work experience, recovery capacity, knowledge of proprietary information and data, and intrinsic knowledge of processes, procedures, inventories, and systems—not to mention the costs of hiring, training, equipping, and supporting—the personnel in your organization may, in fact, be one of your largest single financial investment and asset resources. One lesson of both the 9/11 attacks and Hurricane Katrina is that even if your data are sufficiently backed up, good planning requires an alternative workplace with backup systems. If you lose all or a significant part of your workforce to displacement from the area, death, physical or emotional injury, or disrupted work lives, the survival of your organization is at risk.

No disaster preparedness planning can be considered thorough unless it specifically includes detailed consideration for the health, safety, and welfare of the people within your organization. Your plans must address all levels of their well-being. Take all reasonable steps to ensure not only the physical safety of your people under all contingencies but also their emotional, mental, economic, and work life continuity needs.

PERSONNEL SECURITY NEEDS

One way to organize planning for personnel security needs is to use the Chandler personnel security needs pyramid. The model indicates that the urgent foundational needs are the priorities of providing for and maintaining the physical safety


Work-Life Continuity
Economic and Financial Needs
Psycho-Socio-Emotional Well-being
Physical Safety and Personal Security

Chandler Personnel Security Needs Pyramid © (2004), Robert C. Chandler, Ph.D.

and personal security of all employees and other people within your span of control. Keeping people safe or moving them to safe locations from a wide variety of possible threats is the fundamental goal of planning. Safety is both a short- and long-term goal. Physical safety and security can be ensured only with a dynamic process that is flexible to changing circumstances and evolving situations.

The personnel security needs pyramid places the psychological, sociological, and emotional well-being of your personnel as the next priority. The psycho-socio-emotional distresses can come from various forms of emotional trauma and disorientation. Devastation and work disruption can exact a significant toll on your workforce's mental health and well-being. Consider the various threats and plan safeguards (mitigation and recovery), including strategies for posttrauma comfort. Also anticipate employee concerns about family and loved ones affected by the disaster, and how these concerns will impact individual work performance.

Employees can focus on your business operations and crisis response only when they are confident that their families and personal lives are secure during the event. If they are worrying about who will pick up their kids from school or unable to verify the safety and well-being of their loved ones, then they will inherently have a lack of focus on your business operations. Crisis preparedness for business is built on a foundation of individual employee family crisis preparedness. It is a good business investment to help your employees, particular key crisis managers, prepare for crisis events in their homes, in their automobiles, and among their immediate family. Every one of your employees should have a family crisis plan that covers all of the same basic issues that your business plans cover, except on a smaller, more personalized scale.

The third level of security planning for personnel concerns their economic and financial needs. It may not be something that you want to think about in the aftermath of a terrorist disaster. Protecting your personnel will require that your payroll be disbursed, ensuring that bereavement benefits are delivered, alternative transportation is arranged, company credit cards still function, emergency checks are cashed, and insurance claims are appropriately addressed. Do your employees have emergency cash on hand until the banking system is back online (or transportation allows access to an ATM)? Should your company provide for this need (such as cashing checks or providing cash advances for employees)?

The final level of need includes necessities centered on work-life continuity. During crises, most personnel simply want to "do something/do anything" in order to feel that their activity is appropriate and useful. However, after the adrenaline fades and all other security needs have been met, the typical employee senses a need for a resumption of work-life continuity. You should address concerns about when and where the normal work routine will resume, what the company will do about lost data, whether there is going to be a temporary workstation or facility, and expectations about normal events (meetings, deadlines, etc.). Your personnel ultimately need assurance that work life has returned to normal after these crises or disasters and that you understand their anxiety in dealing with different parameters for the production of work.

Clearly, personnel security needs is a complex issue. Key personnel security concerns include (1) emergency first aid preparedness, (2) evacuation/shelter-in-place planning, (3) addressing posttraumatic stress, and (4) recognizing symptoms of stress trauma.

Emergency First Aid Preparedness

When a workplace emergency occurs, injuries are likely to occur. History has shown that many injured people can be assisted with basic first aid. Often during an emergency situation, emergency responders will be delayed, and critical first aid will not be readily available unless it can be provided in-house. In this case, the first aid responder can supply the initial assistance that may help the victim survive until trained emergency medical technicians arrive. Providing first aid should not be an expensive proposition. You are not required to hire licensed physicians or nurses. The contents of your first aid kit, an essential element of emergency medical response, should treat the types of injuries that might occur in your workplace and suit the expertise of the first responders providing initial care and relief. Cuts and burns often represent the greatest exposure in the workplace, so ointments and bandages are a minimum requirement. Another supply kit to consider is an expanded version of the traditional first aid kit; this emergency kit contains the basic supplies and necessities to ensure safety, comfort, and care if your personnel were inaccessible to paramedics or emergency responders for a period of time. Experience during Hurricane Katrina and in the Oklahoma City, World Trade Center, and Pentagon attacks has shown that these "emergency kits" are a reasonable provision to better ensure the health and well-being of personnel. Emergency kits should be prepositioned at the employees' workstations, in their personal automobiles, and in each of their homes.

Evacuation/Shelter-in-Place Planning

One critical decision that frequently must be made quickly during disasters is whether to order a building evacuation or to lock down personnel and provide a shelter-in-place order. Evacuations may be appropriate for certain threat situations. Your crisis team needs to develop various scenario protocols in advance of these crisis events. Once a decision to evacuate is made, the management of a fast, efficient, and safe movement of personnel out of a building is a difficult assignment for the crisis manager. During an actual emergency event, people often become disoriented and confused. Disruptions to internal communication systems can further complicate evacuation. When considering the evacuation of a building, special consideration must be given to persons with disabilities (e.g., those with hearing limitations not being able to hear an alarm; those with visual limitations not being able to exit via a safe passageway). Employees and visitors with certain mobility limitations may find it difficult to leave the building, especially if the elevator is not available. You have a responsibility to provide a safe evacuation for all employees including those with disabilities. Determine the types of scenarios in which you would order an evacuation and which specific exit routes to use, and which scenarios would lead you prudently to issue a lockdown or shelter-in-place order.

Addressing Posttraumatic Stress

Responses will be varied and be based on a number of factors including the individual's pre-event history, the nature of the event, and the postevent environment. You can mitigate some of the effects by having an adequate response plan as well as acknowledging the need for attention to the psychological reactions. The levels of posttraumatic stress are directly related to the level of severity of the event. However, regardless of severity, all crisis experiences can potentially impact employees in a significant way. The emergency response team must be equipped to administer a degree of "psychological first aid." Include in your plan the mechanisms in place to allow employees a place to discuss what they have experienced with an empathetic listener. Early intervention and availability of assistance must be the first priority. Look for signs of anxiety and stress. Outsource cleanup activities and suspend or move operations to a temporary location while facilities are repaired and cleaned. Create a temporary crisis counseling center and/or hotline so that employees can receive professional assistance. Debrief the situation at a mandatory session where management or leaders of the company can personally address the employees and explain the plan for the future.

Recognizing Symptoms of Stress Trauma

No single set of behavioral indications of critical emotional or mental stress trauma exist, nor is there a universal timeline or experience pattern for those affected by crises and traumatic events. Personnel who are directly injured or witness harm inflicted on others can be affected by those experiences. Law enforcement and other emergency responders experience distress. Some post–9/11 studies have suggested those who are essentially unconnected to terror attacks and geographically distant can also have negative traumatic experiences from simply "witnessing" the attacks on news media coverage. Certainly those who come face to face with the tragedy of terrorism and those who have coworkers and friends injured or murdered are at high risk of emotional or psychological distress.

Not all distress is equally debilitating. Some mild forms of distress may not be manifested in easily recognizable ways. However, as the significance of the distress increases, it is more likely that those affected will show observable signs. Trained and qualified personnel should investigate these indications. However, everyone in your organization should be alert to warning signs and be knowledgeable of how to initiate appropriate protocols to assist those who need help and support. Anything that appears out of sync with "normal" behavior patterns should be considered a potential warning sign. Obviously, those who are most familiar with individuals may best recognize any such warning sign. Further, other indications can be common, such as the following: recurrent thinking about the attack, sleep pattern disruptions (including nightmares), anxiety about routine activities significant enough to interfere with performance, atypical anger or irritability patterns, depression, memory loss, excessive crying, new physical dysfunction (seizures, twitches, pain, heart rate increases, nausea or vomiting, teeth grinding, dizziness, profuse sweating, etc.), cognitive disruptions (loss of decision-making skills, inability to focus, inability to engage in coherent conversation, etc.), or other dysfunctional behavioral signs. Your employees should have basic training in recognizing any significant behavioral changes in the aftermath of a major terrorist attack or event.

CRISIS COMMUNICATION PLANNING

A crisis communication plan provides policies and procedures for the coordination of communication among key relevant individuals within the organization, as well as between the organization and external audiences including emergency responders, the local community, family, the news media, and the general public in the event of a disaster. The goal of a crisis communication plan is to articulate guidelines, procedures, options, and available resources for a variety of disaster situations. A crisis communication plan should provide instructions and guidance for all aspects of communication during a disaster—as the road map or game plan that guides the communication during and after a disaster. This road map helps to protect and aid those affected by the disaster.

Typically, crisis communication plans do the following: stipulate how information is to be gathered and processed (e.g., incoming communication and information processing/decision making); identify key constituencies that should be informed about the disaster situation; provide a specific plan (with backup stipulations) of how to notify, alert, and inform each target constituency; offer a set of prepared message maps to guide the creation of messaging appropriate for each disaster scenario and target audience; have procedures to minimize rumors, misunderstandings, and misinformation; and contain protocols to ensure appropriate and efficient communication during and after a disaster. Because crisis communciation is an essential part of disaster recovery management, an effective crisis communication plan addresses (1) communication messages, (2) communication technology disruptions, (3) automated emergency notification systems, and (4) media relations.

Communication Messages

The basic underlying purpose of messages is to seek an object for information, refusal, provision of information, indications of agreement, or social engagement. Think of the goal of the childhood game “telephone”: to pass the message from the beginning of a line to the end. Although the entertainment of this game is that the message is never the same at the end, it’s not so funny in real life. Messages are sent to the receiver by verbal and nonverbal behaviors. Nonverbal messages may be a simple nodding of the head in agreement or the rolling of the eyes in disbelief or annoyance. During a crisis, it is imperative to minimize misunderstandings from verbal and nonverbal behavior. The burden is on both the initiator—to verify that the message is understood correctly—and the receiver—to clarify questions. Providing an understandable message requires being clear and concise. Hindrances to communication include poor word choice, too much or too little information, poor construction, and technical jargon.

Communication Technology Disruptions

Without electricity and support utilities, many of your otherwise “dependable” communication technologies may be down as well. If your crisis response relies on functioning landline or cellular telephones or the Internet, you may have to communicate effectively without these channels. Traditionally, in large-scale disasters, alternative communication technologies have been able to “fill the connection gap.” In major widespread natural disasters, global amateur radio operators have consistently been able to maintain communication connections to entire geographic regions that would otherwise have been isolated and cut off from communication. This may not be an appropriate “backup” for your crisis communication needs, but carefully consider which alternatives would be best for your circumstances. Your own business may consider small investments in these dependable alternative communication technologies as a last resort contingency.

Ask these key questions about alternative communication technology when building your crisis communication plan: Whom do you need to communicate with in each crisis scenario, and will this technology enable your connecting with these key contacts during and after the crisis? Does this technology have the capability to communicate (voice, data, etc.) the information you need relayed under crisis conditions (alternative power, range, frequency, overcome typical interference, etc.)? Does it require knowledge, skills, or abilities that personnel who are available during crises possess? What equipment and costs are required to have a complete “two-way” communication connection via this technology during a crisis? Can your personnel operate this technology “in the open” (no privacy of communication) during a crisis (particularly the public bandwidth and frequency applications)?

Automated Emergency Notification Systems

Sometimes you must get urgent emergency warning or alert notification messages out to appropriate targeted audiences rapidly. Years ago, “telephone calling trees” were used to notify a large number of individuals. However, these inefficient approaches were prone to errors and had many shortcomings when you needed confidence that your messages were reaching the right people right away. The emergence of automated notification systems addresses these flaws. Automated notification systems, also known as mass notification systems, are faster, more accurate, more effective, and often much less expensive than manual communication systems. They deliver a large volume of text, voice, or data messages to a potentially large audience in an extremely short amount of time.

Normally, they can send messages through multiple communication channels—not only by telephone but also by e-mail, pager, fax, instant messenger, PDA, and other channels. These systems accomplish this feat by utilizing computing, wireless, and telephony technologies that have matured in the last few years. Although nearly all automated notification systems try to address the challenges identified above, they do come in a variety of basic architectures and configurations. Some are operated internally by the businesses that use them, whereas vendors operate others. Three popular categories of notification systems available today are “box” solutions, application service providers, and web-native application service providers. Disasters create demands that must be actively managed in order to mitigate or prevent catastrophic physical, financial, or reputation harm. An automated communication system should be evaluated for its inherent ability to help a crisis team perform its management tasks. For more information on notification communication, refer to the Guidance Appendix.

Media Relations

Disaster recovery managers have a lot to keep track of during emergencies and crises: the safety and well-being of people, keeping mission critical operations up and running, protecting property and resources, keeping senior management happy, ensuring ongoing profitability, and the general reputation of the company, to name just a few. They certainly don't like the responsibility of having to interact with the news media during their continuous operations.

Media Relations

Whereas most disaster recovery managers already know how to handle the recovery processes for facilities, operations, and systems, many are unprepared to effectively speak to a reporter, provide a successful interview, or conduct a field press conference that builds a positive reputation for their operational competence. Far too many disaster recovery managers don't know how to act as a spokesperson, conduct a news briefing, or handle a barrage of media inquiries when public relations people are unavailable and the media await a response. Disaster recovery managers must have basic working knowledge and abilities for working with journalists and the news media, as well as some critical skills in the role of spokesperson with general media training to complement a well-developed communication plan.

Missteps in working with the news media during a disaster or a disaster recovery operation can wreak havoc on a company. Loss of support from investors and customers can mean economic chaos. Ensuring the consistency of your corporate identity and reputation is one of the major goals of ethical continuity. You must be prepared to communicate effectively with all of these audiences to ensure the continuity of your operations. All of these goals depend on effective and successful communication. Communication should not be left to happenstance; successful crisis communication requires a strategic commitment and substantial efforts to prepare and implement, as well as a focus on communicating (building) a positive image and reputation.

(continued)

Survival of the media barrage during your disaster recovery operations requires getting your message to your key constituent audiences as well as the general public. Whether you meet the demands of reporters depends to a large degree on your communication during disaster recovery operations under less than ideal circumstances. Efficient communication, information coordination, and message control during and after disasters are achievable only to the extent that you have a sound and workable plan for communicating during the recovery operations. Hopefully, you developed a comprehensive communication plan as part of your overall business continuity planning efforts. In any case, a crisis communication plan should detail how you or your unit plans to interact with the news media as well as employees, families, customers, the local community, emergency responders, and government and in the aftermath of the crisis, whatever its cause. Disaster recovery managers need immediate and reliable intelligence during critical events and must provide feedback to senior management, utilize all relevant information for ensuring continuity of business operations, and communicate with stakeholders. The public, in general, and the news media, in particular, require specific information during and after such crises. It is important to communicate with the public frequently through the news media. Contact with the news media is a challenge for which it is essential to be prepared. Your customers, investors, employees, and other stakeholders will have questions about the impact of any disaster to your ongoing operations.

Yet, at the scene of the disaster, the news media are ubiquitous and a situational reality that every disaster recovery manager eventually has to confront. Working in close cooperation with corporate public relations and public information officials can assist the disaster recovery professionals in managing this challenge. In many cases, these resources help do the heavy lifting of media relations work. However, at certain times it is essential for a disaster recovery manager to interact directly with journalists and the news media. For more information on media relations, refer to the Media Relations box and the entry Crisis Spokesperson.

CONCLUSION: READINESS, TESTING, AND ONGOING PLANNING

Because disaster management preparedness is never really finished, it is essential to test, revise, and continuously update your planning efforts. One mile marker for disaster management planning is establishing agreements with providers who can assist you in an emergency and in recovering your operations. Without this external help, arranged in advance of the next disaster, the only companies to get needed goods and services will be those willing to pay the highest price in a "seller's market." Prepositioning, prior commitments and agreements, and prearrangements are a sign that your planning is moving forward.

No disaster management plan can be depended upon if you have not tested, practiced, and revised it. Although you are never quite finished with your plan, don't wait for an actual disaster to give it its first test. Testing, revising, and updating are key ongoing activities to ensure vigilance in your disaster management planning. Train employees directly as to how they should react in various situations. Practice the plan in simulations, with tabletop exercises, and in full mock drills. Although it will never be perfect, no matter how many times you go through it, after each test debrief and revise your plans.

Preparing for catastrophically disruptive events is a vital and important series of tasks on which there is much at stake, including financial, continuity, reputation, and the health, safety, and even life/death of people. The challenge for disaster management planners is that each of the many different types of threat risks and possible categories of disasters requires unique response plans to mitigate its impact and expedite recovery. It is crucial for an organization to develop plans that review areas of vulnerability, to prepare to survive the worst-case scenario, and to get back to business as usual as rapidly as possible.

See also Crisis Spokesperson; Ethics as a Business Security Concern; Insider Threat; Reputation Management; Shelter-in-Place; Exercise and Training Basics; and Types of Crises.

NOTE

[1] National Commission on Terrorist Attacks, *The 9/11 Report: The National Commission on Terrorist Attacks Upon the United States* (New York: St. Martin's, 2004), p. 295.

BUSINESS CONTINUITY

Geary Sikich

I define business continuity as "All initiatives taken to assure the survival, growth, and resilience of the enterprise."[1] This definition can be used to avoid two common problems in business continuity: (1) its failing to keep pace with changes in business and (2) its not being connected to the organization's strategic plan.

A MISGUIDED FOCUS ON TACTICS

Most business continuity is approached from a tactical orientation meaning that business continuity focuses on the mechanisms that support the business—workstations, information recovery, response level measures—rather than on the business. Examples of the tactical-level focus include standard models such as National Incident Management System (NIMS), Continuity of Operations Plan (COOP), and Living Disaster Recovery Planning System (LDRPS). A better way to ensure continuity is strategically—by taking the long view and doing what it takes to preserve the business, not just its components. That long view naturally takes tactics into consideration.

The general model for business continuity planning starts with some form of analysis, generally referred to as the business impact assessment or business impact analysis (BIA). However, this analysis rarely looks at any external factors, such as customers or cross-functional dependencies. Instead, it typically produces a "false positive" report. Although it may discuss protecting infrastructure, it does not address loss of customers, critical human capital assets, and the like.

A false positive is created when people ask a question that, when answered, provides them with a sense of comfort that does not reflect the actual state of affairs. By asking the wrong questions, we are getting the wrong answers. People have false sense of security because they think their business continuity efforts are complete. An example of a false positive is found in a *CSO Magazine* article entitled "Disaster Preparedness." Jon Surmacz noted that about two-thirds (67 percent) of *Fortune* 1000 executives say their companies are more prepared now than before 9/11 to access critical data in a disaster situation.

> The majority (60 percent) say they have a command team in place to maintain information continuity operations from a remote location if a disaster occurs. Close to three quarters of executives (71 percent) discuss disaster policies and procedures at executive-level meetings, and 62 percent have increased their budgets for preventing loss of information availability.[2]

The executives surveyed view the ability to access information and maintain its availability as business continuity. But what about the loss of personnel, loss of facilities, loss of access to normal business environments, or any other potential problems that could be encountered in a disruptive event? In today's world, we face everything from natural disasters to cyber security issues. Businesses are so interconnected that new solutions have evolved to address the complexities. A few years ago no one had ever heard of customer relationship management (CRM), enterprise resource planning (ERP), supply chain management (SCM), and a host of other terms that are commonplace today. Yet they represent relationships that must be preserved in the event of a disaster.

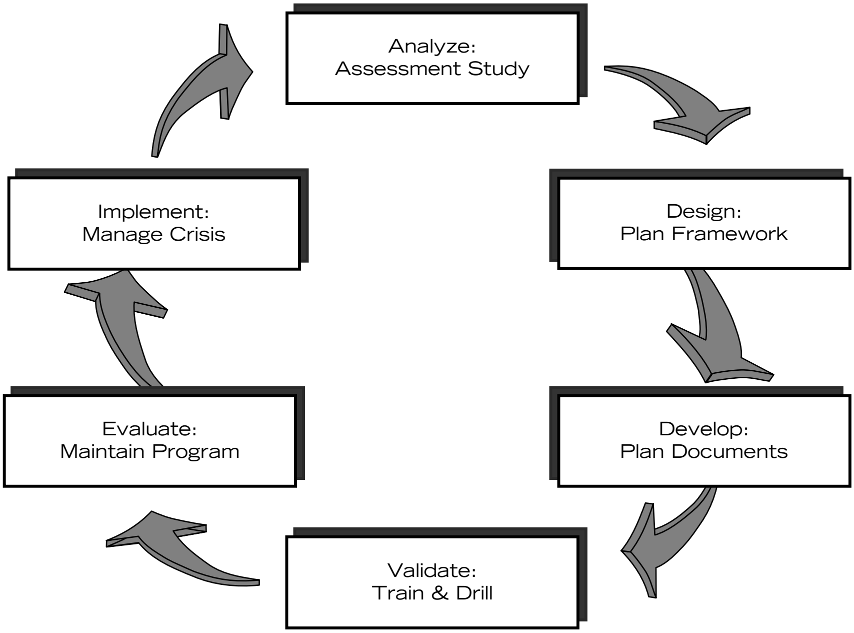
If organizations continue to ask the wrong questions, decisions will be made based on the wrong answers. Corporate management must learn to ask the right questions. The fate of every organization depends less and less on those who can solve "canned" problems, and more and more on critical thinkers—smart thinkers—who can define, and even redefine, the hellishly difficult problems facing us.

THE CONTINUING EVOLUTION OF BUSINESS CONTINUITY: IS YOUR ORGANIZATION KEEPING PACE?

Business has changed as longer supply chains create interdependent systems and business is practiced at a much faster pace.[3] Business continuity planning does not always reflect these changes but, done right, it can.

Business continuity planning generally consists of distinct phases that delineate the progression for development of the plan. As depicted in figure below, this is, ideally, a recurring cycle.

Business continuity planning can be generally broken down into three general levels or constructs: tactical, grand tactical (operational), and strategic. The tactical level covers work groups, departments, teams, and first responders—basically small units. The grand tactical level concentrates on business operations,



The Recurring Business Continuity Planning Cycle divisions, and business units—basically a cluster of tactical-level entities under the supervision of a higher level of authority. Grand tactical can also relate to geographic area of coverage for some organizations. The strategic level is the typical corporate level—boardroom, CEO, and so on. From a governmental perspective, tactical equates with local government, grand tactical with state government, and strategic with federal government.

As noted, we need to rethink how we define significant disruptive events. Our focus must expand beyond the tactical issues to include more of the grand tactical and strategic issues facing our organizations. We do the tactical very well, but it's time to step up the "value proposition" of business continuity.

All three of these planning levels are important to a company for different reasons, yet each has a unique level of importance and impact on the company. The goals of the three levels of planning are entirely different and therefore must rely on different methodologies to produce effective plans.

At the strategic planning level, a combination of past performance of the company, coupled with external information, becomes the starting point for the planning process. The senior executives deduce what performance factors must be met in order to stay competitive in the market. At this level, the distribution of company assets is also assigned. An example would be how much money will be dedicated to current operations, market expansion, new building construction, and possible new product development and distribution.

Moving to the grand tactical (operational) level, management starts with predetermined budgets and existing procedures. It must develop the efficiencies to enable delivery of the company goals in its area of responsibility or current operations. The tactical level of planning is the intermediary; it is responsible for the distribution of budget dollars throughout the company as well as for finding efficiency factors that will impact supplies and suppliers. In all three cases, the starting point, or foundation, for that level of planning is different. At the strategic level, the goals are defined. At the tactical level the goals are nonnegotiable and asset distribution is the point of flex. At the grand tactical (operational) level, the assets are defined and the processes and procedures are changed to meet the tactical-level directives.

Just as the planning protocols for a company have different formats and objectives, so also do recovery/restoration planning programs. Disaster recovery planning is generally oriented to the tactical level, because it is the preparation necessary to continue key operations under a variety of possible circumstances. Problems and issues at this level are seldom life threatening to a company, though they can have substantial financial impact. Business continuity planning as it is currently practiced is generally also at the tactical level. Seldom is it found among the company's strategic goals; more often than not it focuses on internal procedures. Just as grand tactical (operational) plans redistribute company assets to achieve strategic goals, so too should business continuity plans be designed to redistribute company assets to achieve these same goals, but in a different work environment. This means that existing processes and procedures cannot be the starting point of a business continuity plan. The starting point, rather, should be the same as that of grand tactical (operational) planning—the organization's strategic goals. The internal processes and procedures and even the company configuration will all change during and after a disruptive event (crisis) as a result of customer demands, investor values, and competitive forces.

Traditional business continuity planning usually starts with identifying the risk factors. These are, however, in most instances limited to systems risk factors that could impact the company. An analysis—a business impact assessment—of those risk factors then follows to quantify their effect on the company. This information becomes the foundation for the business continuity plan. If we start with the assumption that a company has a strategic plan, it is logical to conclude that the business continuity plan is an extension of that fundamental business plan that enables a company to achieve its strategic goals under extraordinary conditions.

The current process of developing business continuity plans (BCP) generally does not take into account certain fundamental issues in the corporate planning process. Most BIA efforts take anywhere from three to nine months to complete. In conversations with BCP planners, six months is the most common time frame for the completion of this effort. After that time, all of the collected information must be synthesized, organized, and documented in the form of a business continuity plan. A BCP, by definition, should support the company's strategic plan. The reason planners today accept this "traditional process" is because few if any of the current business recovery planners or consultants in this field have ever written a strategic plan for a corporation. If they had, they would understand that the shelf life of a strategic plan is three months, six months at most. After that time, changes in the market, customer priorities, competitive forces, or financial issues cause the plan to change. If currently accepted practices take three to six months just to quantify the impact to the company of certain risks, and additional time is needed to formulate a "business recovery tactic" in the form of a BCP, we are faced with the very real problem of information value. How effective can a business continuity plan actually be when the information it is founded upon is out of sync with the company's strategic plan?

The other fundamental flaw in this process centers on the fact that the BCP is supposed to support the company's effort to achieve its strategic goals under extraordinary circumstances. However, I have not seen any BCP that identifies the company's strategic goals as part of the plan. The concentration in the BCP is the perpetuation of internal process within the company, not the achievement of goals. If the BCP is, in most instances, out of date with current strategic factors impacting the company, it is fair to question the effectiveness of the operations that are being recovered and their current value to the company. The BCP process of collecting information within the company to identify mission critical operations illustrates a misunderstanding of the company's planning process. A company starts its strategic planning process externally. It examines the market (customers, competitors, and product value), as well as investors and what they are looking for, to determine how the company must perform in order to gain and keep investors. A company does not start by examining the current internal capabilities and process to deliver its service or product.

Using mission critical operations as the basis for a planning effort can lead to some costly problems for a company. If a process or procedure is valuable today, will it necessarily be valuable after a disaster? Because the current thinking of BCP planners is yes, they start their planning effort with this assumption.

All business concepts and protocols evolve over time. Most of this evolution is driven by the dynamics of the market, but in some cases it is driven by the expanded knowledge and need for more sophisticated protocols to be effective. At first, IT business staffs tried to codify the process used within their operations as various forms and methodologies that would be applicable to the whole company. After several years, the lack of acceptance of these methods resulted in a change of direction. From disaster recovery planning, the process evolved into business continuity planning. Clearly this orientation was far more extensive in considering business issues. The only real problem with this evolution was that it was founded not in the business of the company but instead in the procedures of the company, just like its predecessor, disaster recovery planning. Although the process title had changed, the fundamental output remained principally unchanged.

As more planners from other fields such as strategic planning enter the field of survival planning, new experience is leading planners to the understanding that the tactics necessary to survive a catastrophic event must be addressed with the same orientation as the company's actual business plan. If the company does not achieve certain strategic goals, it will not survive in the market. So the crucial concepts in business planning are equally important in the business continuity plan.

So today there is a slow and uncomfortable movement into an expanded realm of planning for traditional business continuity planners. As they move away from a protocol that was effective for operational responsibilities and move up into more complex issues that need to be addressed for company survival, they must reorient their thinking. Now the driving forces are the achievement of "strategic goals," using adjusted tactics that are necessitated by some form of disaster. New tactics will have to evolve to support the company goals and protect the customer and investor base, which is the financial key to survival of the company.

THE BUSINESS IMPACT ASSESSMENT PHASE

The business impact assessment phase (BIA) is characterized by identifying critical business processes and establishing recovery time objectives and recovery point objectives. The warning signs are clear to the observant. But most, if not all, BIA methodologies tend to miss the broader issues because they focus primarily on the recovery of systems, not of the business as a whole. For example, say you are assessing the business impact of the loss of a critical system, such as inventory management. You may come up with several potential impacts that result from the loss of this system. But if you do not take into account that the company may lose a warehouse and be unable to fulfill customer orders, then the BIA has failed to assess the business impacts for the client properly and resulted in a false positive.

Failures to assess unsafe operating practices and to address known hazards, threats, vulnerabilities, risks, consequences, and inadequate reporting mechanisms, are but a few of the indicators of an inadequate BIA. Lack of an integrated BIA further exacerbates the creation of false positives. The BIA is critical for the next phase in continuity planning: strategy evaluation and selection.

Following are twelve questions from a sample questionnaire I have used as a simple assessment process. You still need to determine what your enterprise requires in terms of the assets that support the business (facilities, workstations, information systems, etc.), but these questions may pave the way to get senior management buy-in for the BCP.

1. What Is a "Crisis" for Your Company?

Typical Answer

A crisis is any *critical incident* that involves death, serious injury, or threat to people; damage to environment, animals, property and/or data; disruption of operations; threat to the ability to carry out mission; and/or threat to the financial welfare and image of the company. A crisis is an unexpected event or series of events that spirals out of control, interrupts normal operations, and causes intense and unwanted public scrutiny that harms or threatens to harm an organization's reputation.

While these definitions are good, they are process focused and therefore limited. Recognizing that a crisis is any event that threatens the existence of the enterprise or the ability of the enterprise to conduct its normal operations offers a broader, less process-focused perspective.

The following definition of *business continuity* does not attempt to define *crisis*. Rather, it focuses on goals and objectives instead of problem identification:

> All initiatives taken to assure the survival, growth, and resilience of the enterprise—this means *not merely thinking about the plannable or planning for the unthinkable, but learning to think about the unplannable.*

We now know what to measure, we know the current performance, and we have discovered some problem areas. Now we have to understand why problems are generated and what are their causes.

2. What Is the Single Highest Probable Failure Factor for Your Business?

Typical Answer

Terrorism, technology failure, and natural disaster.

What about competition? A competitor will put you out of business faster than a natural or man-made event. In *Management and the Activity Trap*, George S. Odiorne points out that many organizations become so enmeshed in activity that they lose sight of their goals, and the activity becomes an end in itself. Unquestioningly continuing activities from past years, lacking clarity about objectives, and losing sight of the enterprise's overall purpose often lead to the enterprise's failure. Why not take the most important problem and truly analyze it?

A management system should provide a framework for picturing the major factors in the situation as an integrated whole. It should be realistic. It should simplify the complex rather than complicate the simple.[4]

The disaster won't necessarily do you in. But a competitor who takes advantage of your poor planning, including disaster planning, might.

3. How Will Your Company Pay for Its Next "Crisis"?

Typical Answer

Business interruption insurance.

Can you afford the inevitable delays in getting cash when it is truly needed? Do you know what will be excluded from your claim? If you are to survive the crisis, your enterprise has to be able to meet customer and marketplace demands. If you cannot provide the products or services, you will not have the customers for long.

4. What Does Your Current Business Interruption Insurance Policy Cover?

Typical Answer

Not sure. I have not read the policy and do not know where it is located or what coverage we have.

Read your policy and understand the exclusions!

5. Do You Know What Contingent Business Interruption Insurance Is?

Typical Answer

I don't have a clue.

Contingent business interruption insurance is an extension to other insurance that reimburses lost profits and extra expenses resulting from an interruption of business at the premises of a customer or supplier. The contingent property may be specifically named, or the coverage may blanket all customers and suppliers.

6. Should a "Crisis" Materialize for Your Company, How Will It Achieve Its Strategic Goals and Corporate Objectives?

Typical Answer

Not sure. I guess that we will adjust them based on the situation.

Is your plan focused on mission critical activities or—better—mission critical goals and objectives ? The "business of the business" has never been part of the planning process, because planners never recognize they are focused on the company's activities rather than its objectives. Until planners understand and recognize the difference, their company will be limited in its business resiliency capability.

7. How Would a "Crisis" Reshape Your Company?

Typical Answer

Not sure. We might have to divest some assets and restructure.

What is really required is a change in focus or reference points—more ownership of the problem, linked to product and/or service life cycle instead of focusing on point-specific and event-linked plans.

8. Does Your Corporate Culture Embrace Contingency Preparedness as a Way of Doing Business, or Is This Perceived as an Adjunct to the Business of Your Company?

Typical Answer

Planning for contingencies is like regulatory compliance; it is something that you do but do not integrate into business operations.

Have a compelling story—know what drives the business, how "core business" is defined, and how you'll keep it going in the event of a disruption.

9. Has Your Company Addressed Human Capital Utilization During a "Crisis"?

Typical Answer

Current plans do not identify the consequences of loss of personnel.

Traditionally, human resources (HR) has had a limited role in crisis management activities, mainly to address "humanitarian assistance" aspects of crisis response. However, when starting to rethink HR's role in today's global environment, we see that HR's crisis management role is more than humanitarian assistance.

HR's role should focus on a comprehensive structuring of initiatives designed to establish and maintain resilience between and among all the touch points of the enterprise. Human factors must be taken into consideration in eight key areas:

- *Management:* Decision making regarding the handling of the event
- *Planning:* Short term and long term; effect on product/service offerings; client impact; human capital needs (to include intellectual skill sets, training time, etc.)
- *Operations:* Affected and nonaffected, staff degradation levels, availability of human capital (resource pools)
- *Logistics:* Work site, temporary work sites and supporting logistics (equipment), extended logistics support
- *Infrastructure:* Internal and external
- *Administration:* Support factors
- *Finance:* Short-term dislocation and long-term dislocation, budgets, and so on
- *External liaison:* Communication to stakeholders regarding disposition of the event and human factors considerations

10. How Critical Are Your Customers to Your Company's "Crisis" Preparedness?

Typical Answer

Customers are not critical to company preparedness.

Customers are the lifeblood of the enterprise; without them there is no enterprise. The marketplace will define your enterprise. Therefore, it is imperative to involve customers in your planning process.

11. How Critical Is Your "Value Chain" (Suppliers, Vendors, Contractors, Third-Party Service/Product Providers) to Your Company's "Crisis" Preparedness?

Typical Answer

Third-party entities are not included in our contingency planning process because they are outside the scope of our plan.

If customers are the lifeblood of the enterprise, your value chain enables you to meet their demands. Unless you have a totally vertically and horizontally integrated enterprise (in other words, a monopoly), you cannot survive without the participation of the value chain in your planning process.

12. Are Your Product/Service Offerings Immune to a "Crisis"?

Typical Answer

Not sure.

When was the last time that you bought a box of carbon paper for your typewriter? Have you ever used a typewriter? The advent of the computer ended the era of the typewriter and subsequently ushered in the death of an industry segment that was not in competition with the computer—carbon paper manufacturing. Ask yourself, will my product/service continue to be in demand in a changing marketplace? Becoming a risk intelligent organization—one that learns as much as possible about the nature of risks, threats, hazards, and vulnerabilities—allows you to develop continuity strategies that facilitate the survival of the enterprise.

STRATEGY EVALUATION AND SELECTION

If the results of the BIA do not include an assessment of broader business issues, strategy evaluation and selection becomes an exercise in futility. Typically, strategy evaluation and selection is based solely on the results of the BIA. If the BIA has produced a systems impact assessment rather than a business impact assessment, strategy evaluation and selection will focus on recovery time objectives related to systems. This means that selection will focus on hot –sites, not on warehouse space. What do you do with your inventory when you move to the hot site?

Make sure to address the broad issues. Then select a strategy and proceed to develop a business continuity plan to implement that strategy.

BUSINESS CONTINUITY PLAN DEVELOPMENT

The plan is one of the most critical documents. And yet, it is most often overlooked because it is not integrated into how the company does business.

As such, the final BCP often ends up on a shelf collecting dust. It quickly becomes dated and is essentially a liability document because commitment identification, tracking, and documentation are not performed. Personnel with responsibility for implementing the plan more than likely do not receive the required training to do so. And, if they have to implement the plan, they may find that the disruptive event is not one that the plan covers. For instance, does your BCP address the issue of eminent domain? Refer to the BIA, and then create a workable plan that ensures the continuity of your business—not just its systems.

Business continuity planning is in fact an adaptation of current tactics to deal with new barriers that have limited the company's ability to achieve its strategic goals. As new tactics are deployed to achieve these goals, new operational procedures will develop to support these tactics. The whole planning process will be driven from the top down, not in traditional terms of bottom up. The only mission critical operations will be new operations defined by new tactics that ensure the achievement of the company's strategic goals. Current procedures will give way to new modified procedures that are needed to support current customers and investors.

The ability to flex and evolve into new methods of supporting current goals requires a new level of interaction within the company. Failure to develop this capability limits a company's ability to respond to new demands and problems that have resulted from a disaster. This can be every bit as potentially life threatening as failure to respond to competitive pressures in the market.

BUSINESS CONTINUITY PLAN VALIDATION (TESTING) AND MAINTENANCE

Once the plan is created, it's important to conduct training, validation (testing), and plan maintenance. Most organizations do none of these, because they fail to incorporate the plan into a way of doing business. The plan becomes an addition to the business, not integrated into daily work. If the plan is primarily systems based, it is further divorced from the business. Silos are created and critical planning constructs are not shared. As mentioned above, the plan becomes a liability document. Just think of all the well-intentioned commitments that you make as you develop your plan. You cite in the plan that you will train, conduct simulations, have set aside equipment and facilities, and the like. Have you ever assessed what you have committed to in the plan? Can your organization actually fulfill the commitments it has made? Are you documenting and tracking commitments? It is important to answer these questions.

CONCLUSION

Management today has the responsibility to protect the organization by facilitating total continuity planning and preparedness efforts, not just systems continuity. Market research indicates that only a small portion (5 percent) of businesses today has a viable plan, but virtually 100 percent now realize they are at risk. Seizing the initiative and getting involved in developing a total business continuity plan can prepare an organization to respond to, manage, and recover from a disruptive event that could become a crisis.

All organizations can be hit by some event that could cause a business disruption. Just consider the number of different risks an organization faces. Business continuity provides a mechanism to minimize financial loss; maintain service to customers; and protect people, data, the organization's strategic plan, and its reputation. In short, business continuity is a critical defense mechanism against the negative effects of a business disruption when carefully and thoughtfully developed.

See also Crisis Communication: External and Internal; and Disaster Recovery Management.

NOTES

1. Geary W. Sikich, "September 11 Aftermath: Seven Things Your Organization Can Do Now," *Disaster Recovery Journal*, 15, 1 (2002).

[2] "Safety in Numbers," Disaster Preparedness, 14 August 2003 online at http://www.csoonline.com/metrics/viewmetric.cfm?id=592 (accessed 23 March 2007).

[3] Geary W. Sikich, "September 11 Aftermath: Ten Things Your Organization Can Do Now," *John Liner Review*, 15, 4 (2002).

[4] George S. Odiorne, *Management and the Activity Trap* (New York: Harper & Row, 1974).

RISK MANAGEMENT

Krista Varney

The primary goal of risk management is to ensure nothing "bad" happens. The key component in achieving this goal is the process of identifying, assessing, and addressing risk. It is necessary to understand some of the definitions associated with the process first.

DEFINING TERMS

Risk is the likelihood that something bad is going to happen and the associated impact. It is important to consider risk in the context of probability, not possibility. The fact that something detrimental could happen to key stakeholders (i.e., customers, employees, investors, etc.) of an organization may indicate a need to evaluate risk. However, an organization must understand how likely a stakeholder is to experience this negative event before taking any action to address it. For example, a common fear among the general population is being bit by a poisonous snake and subsequently injured. However, the chances of this actually occurring within a given year are about 1 in 145 million.[1] The probability that a person would come in contact with a poisonous snake during the course of a normal day is very low, and it does not make sense for everyone to keep an antidote in his or her pocket.

Risk assessment is the process of evaluating the likelihood that a negative event is going to occur and the estimated magnitude of loss. The key components of risk assessment include the assets at risk, key objects related to the assets, threats, vulnerabilities, mitigating controls, and loss factors. The definitions and relationships between the components will be covered later in the entry.

Risk management is the process of identifying, assessing, and addressing the risk. As new security threats are identified, the next step is to assess the risk. The best approach for addressing the risk is determined based on the results of the risk assessment, the organization's and its stakeholders' tolerance of risk, and the overall goals and objectives of the organization. The four most common methods used to address risk are accept, mitigate, transfer, and avoid. Once an approach is identified to address the risk, the next steps are to develop a plan and execute it.

Risk management is an iterative process. Because the threat landscape is constantly changing, the risk management process must be able to identify changes in the level of risk. Risk must be measured on a regular basis. Measures in the process are necessary to identify where risk levels have changed, and the decision must be made on how to address any changes in the amount of risk. Part of the process is to build a plan once again and see it through execution.

EVALUATING AND MEASURING RISK

Numerous methodologies have been developed to evaluate and measure risk. Given the nature of measuring risk, none of them provides a 100 percent guarantee of accuracy. It is impossible to predict exactly when the negative event will occur, how often, and the financial impact. Key factors should be evaluated when assessing risk, regardless of the framework being applied.

Risk can be evaluated using quantitative and qualitative methods. Quantitative risk analysis uses mathematical measurements to evaluate the risk, whereas qualitative measures use judgment and reason to measure risk. The difference between the two is precision and accuracy. Quantitative measurement has a high level of precision and accuracy but also usually requires an extensive amount of resources. A best practice for risk analysis is to use a combination of quantitative and qualitative measurements. The goal should be to minimize the level of subjectivity to an appropriate degree. In general, empirical data are not available to serve as inputs to the risk assessment. There may be some data to support incident history and the depreciation value of an asset, but exact data to measure the strength of a control or the capability of a threat are not as easy to identify. Therefore, we may operate within ranges of numbers to allow for estimates that reflect the data that are available and account for the data that are not.

For example, approximately 4 percent of the U.S. population was the victim of identity theft in 2006.[2] You could estimate that between 2 percent and 8 percent of your U.S. customer base, for example, is likely to be a victim of identity theft in 2007. It is impossible to predict the actual number precisely, but using a range around information that is known helps estimate the risk better. From there, you may assign qualitative risk levels to explain the risk. For example, you may, consider a total exposure to loss between $1 million and $5 million high risk.

Once you identify the approach and framework for measuring risk, you can begin the risk assessment process. The first step is identifying the asset at risk. Assets include people, processes, facilities, information, and equipment. In addition to identifying the asset at risk, identify the related components to that asset, because they could be compromised in an effort to reach the primary asset at risk. An example of an asset at risk is customer information. Related components may be the application that contains the customer information, the network and equipment that facilitate the transfer of information to and from the application, a workstation used to access the application, and the customer that the information represents.

It is also necessary to decide which components related to the asset are applicable given the scenario under review. If an attacker trying to use authentication credentials to access a customer's information is the threat, then the customer, the customer's workstation, and the application containing the information may be the three main components vulnerable to the attack.

It is important to understand not only the primary threats to the asset but also the level of force the threats are likely to apply against it and how often. Attacks may come in the form of nature or man-made. An attacker that has significant funding and knowledge about the asset at risk is more likely to be successful than an attacker arbitrarily picking assets to attack with tools commonly found on the Internet.

For man-made attacks, the potential gain of a successful attack compared to the perceived risk is important to consider as well. The higher the reward and the lower the risk of consequences, the more frequently attacks will occur. Natural disasters involve different factors to consider. Location and climate are important to estimate the frequency of a natural disaster. Tornadoes in Alaska would have a lower frequency of occurrence than in Oklahoma.

An asset's vulnerability is determined by the strength of its mitigating controls against the capabilities of a threat. The password of "birthday" is much more vulnerable to a dictionary attack (using an automated tool to use different words in the dictionary to guess a password) than is MbiJ22 (My birthday is January 22). The use of a password phrase is a stronger control in this case, making the vulnerability lower given the same counterforce of a dictionary attack.

The impact of an incident is the final key factor in a risk assessment. Impact may be measured in hours, dollars, or people. Some scenarios may be concerned with how much money would be lost, whereas others may be involved with loss of life or injury. Some factors that may help estimate the amount of loss include the ability to perform key objectives, the effort necessary to respond to the incident, the effort to recover from the incident and return back to "normal," any legal action or government penalties, and reputation.

Overall risk can be determined by calculating the number of times the negative event is likely to occur and the vulnerability of the asset with the estimated impact of an event within a given period of time. The results of the risk assessment are used to determine the course of action to address the risk.

MANAGING RISK

As previously mentioned, risk may be addressed a number of different ways. The most common are to accept, mitigate, transfer, and avoid. Accepting the risk is appropriate when the risk is lower than key stakeholders' level of risk tolerance and does not conflict with the organization's goals and objectives. Mitigating the risk may include adding additional security measures to improve the strength of the controls. Transferring the risk to a third party is another alternative. An example of transferring the risk is to buy an insurance policy. Avoiding the risk is removing the risk all together. For example, an insurance company may determine insuring drivers under the age of seventeen to be very high risk and discontinue offering insurance to those drivers.

Because risk management is an iterative process, the initial assessment and course of action sets the baseline. The process should include periodic reassessments to ensure the risk remains at a level that is acceptable to the organization. Risk tolerance also must be evaluated periodically to ensure changes have not occurred. Tolerance can be expected to change after a significant incident within the organization or in the external environment. For example, risk tolerance has been much lower in the United States since the 9/11 attacks.

A critical success factor for managing risk is the participation and support of senior management within the organization. Senior management should set the guidelines for risk tolerance and participate in the decision making on how to address risk where appropriate. Updates should also be provided on the effectiveness of the controls currently in place and plans to make changes based on changes to risk levels.

CONCLUSION

In summary, risk management is a process that not only involves identifying and evaluating risk but also addressing it and measuring it in an iterative manner. Risk is a measure of probability, not possibility, and is best measured using a combination of quantitative and qualitative measurement techniques. Any framework used to evaluate risk should look at the threat community, the frequency of incidents, the level of vulnerability, and the impact of an incident. Once risk is measured, a decision must be made to address the risk based on the organization's level of tolerance for risk. Common examples of how to address risk are to accept, mitigate, transfer, and avoid. Senior management should be involved in setting the tolerance for risk and the criteria for choosing a method to address the risk.

See also Business Continuity; Crisis Management; Risk Communication; Types of Risk; and Vulnerability Assessment Team.

NOTES

1. National Safety Council, "What Are the Odds of Dying," 2 Aug. 2006, online at http://www.nsc.org/lrs/statinfo/odds.htm (accessed 23 April 2007).

2. Mintel International Group, Ltd., *Security and Identity Theft* (Chicago: Mintel International Group, December 2006), p. 3.

RISK COMMUNICATION

W. Timothy Coombs

The evening of December 23, 1986, marked the worst industrial accident in modern history. The Union Carbide facility in Bhopal, India, released a deadly cloud of methyl isocyanate into the nearby village killing thousands and devastating the environment. The facility manufactured pesticides, mainly the Sevin brand. The investigation found the deadly release should have been avoided. The Bhopal facility had not maintained its own safety systems and had poorly trained its workers. The chemical release killed over four thousand people and crippled thousands more. Over twenty years later the groundwater is still unfit to drink.

So what does this case have to do with risk communication? Union Carbide had a second facility making Sevin located in Hurricane, West Virginia. People feared a Bhopal-style event in the United States. Congress passed the Superfund Amendments and Reauthorization Act (SARA) on October 17, 1986, in large part as an effort to prevent any large scale accidents in the United States. SARA Title III includes the Emergency Planning and Community Right-to-Know Act (EPCRA). EPCRA seeks to increase public knowledge and access to (1) information about toxic chemicals in their communities, (2) the release of toxic chemicals, and (3) the management of toxic waste materials. In addition, EPCRA tries to encourage and support efforts to plan for environmental emergencies. EPCRA created the need for risk communication.

RISK COMMUNICATION: DEFINITION OF KEY TERMS

At this point it is important to define some key terms related to risk communication, and then return to how EPCRA has created the need for organization to be well versed in crisis communication.

Risk is some thing or situation that poses a danger. (Refer to the entries Risk Management and Types of Risk for additional information about risk.) Risk is typically evaluated according to its likelihood of having an effect and the impact of that effect (how bad will it be). *Risk communication* is a conversation about risk between an organization and its stakeholders, typically the community members living near a facility. The focus of risk communication is helping people to understand/evaluate the risk and to manage the risk. Stakeholders need to know the risk they face. Part of that understanding is being able to evaluate that risk. As we shall discuss shortly, evaluation is a very difficult part of risk communication. People also need to understand how to manage the risk. Community stakeholders learn what the organization is doing to address the risk and what stakeholders themselves can do to help manage the risk. Community stakeholders are what are known as *risk bearers*. By living near a facility, they bear the risk of that facility. *Risk management* helps community members cope with the risk presented by the facility.

FOCI OF RISK COMMUNICATION

Risk communication has two main prongs: the first is environmental health (the focus of EPCRA) and the second is public health. Public health tries to educate people about health risks such as the flu or AIDS. Government agencies and nonprofit organizations handle most public health–related risk communication. However, corporations do get involved when the public health concerns can impact their operations. An excellent example is avian flu and the possibility of a pandemic. (Refer to the Pandemics and Pandemic Communication entries for specific information on this topic.) Corporations need to understand how avian flu can affect them, plan for the pandemic, and communicate the plans to their stakeholders. Prepandemic communication with stakeholders is public health risk communication.

TYPES OF RISK COMMUNICATION

Risk communication is a very broad area. We can identify three different types of risk communication based on the primary objective of the communication. The first type of risk communication is when people are not concerned enough about a risk. This is called precaution advocacy. The risk communicator is trying to get people to be concerned and to take the risk seriously. Two examples are attempts to promote inoculations and efforts to get people to evacuate prior to a hurricane. The second type of risk communication is when people are too concerned about a risk. This is called outrage management. The risk communicator is trying to get people to understand the risk is not as bad as they think. Organizations regularly face outrage management, as people tend to overestimate the risks associated with industrial activities. The third type of risk communication is helping people to bear the risk. Organizations face this risk communication task as well. Community members may come to understand the risk, but that does not mean they know how to bear the risk. Crisis communication can facilitate the process of coping with risks.

EPCRA: CONNECTING COMPANIES AND COMMUNITIES

Now let us return to EPCRA, which is built around the concepts of the right to know and the need for emergency planning. People have a right to know about the amounts, location, and potential effects of hazardous chemicals in their communities. This means that organizations must tell community members how much of a hazardous chemical they have, where it is located, and how it could affect people if it were released. The right to know creates the need for risk communication. It is the reason that corporations must begin the risk conversation. If an organization has over a certain level of hazardous chemical, it must report this information to the state emergency response commission (SERC) and the local emergency planning committee (LEPC). The SERC and the LEPC then make the hazardous chemical inventory and accidental release information available to the public.

The emergency planning element of EPCRA is designed to help communities be prepared for and respond to hazardous substance emergencies. The SERC oversees the planning activities of the LEPCs, which are usually county based but can involve smaller geographic areas. They are composed of community members with background in public health, health care, or local industry experience. Organizations are to work with LEPCs to develop emergency plans. The belief is the organizations and the communities are connected. A hazardous chemical incident at an organization can quickly become a community crisis. LEPCs help the community and companies integrate their responses to events. By planning and training together, communities are better able to handle negative events from hazardous chemicals. EPCRA requires that companies notify the LEPC and SERC of any chemical releases. LEPCs can make risk reduction recommendations to companies and are tasked with counterterrorism activities as well.

RISK COMMUNICATION AND OUTRAGE

Leading risk communication expert Peter Sandman has created an equation of risk communication: Risk = Hazard + Outrage. Hazard is the technical or scientific assessment of risk based on likelihood and impact. The focus is on the probability of a risk occurring. Outrage is the emotional and subjective reaction to risk. The focus is on possibility. Consider the following example. Residents learn that a hazardous chemical contained at a facility has a 1-in-250,000 chance of causing a fatality if it is released. People looking at the hazard assessment would place the risk as low. People who hear that the chemical could kill them would place the risk as high. Sandman's point is that risk is much more than a technical assessment of risk. Risk communicators must consider how the community stakeholders perceive and react to the risk if the risk communicators are to be effective.

Originally, risk communication concentrated on hazard through scientific explanations. The belief was that if community stakeholders understood the hazard, they would accept the risk. This belief assumed community members assess risk exactly as scientists do, which is not the case. Community stakeholders bring emotions and perceptions to risk evaluations. Risk often is based on outrage as the risk creates fear and concern. Risk communicators must begin the process of risk communication by understanding the outrage—how community stakeholders assess the risk. The community stakeholders' risk assessment provides the starting point for the risk communication conversation. The risk communicators work with the community stakeholders to reduce the outrage. Risk communicators should avoid discounting outrage as irrational. Outrage is real, as people bring their emotions to the evaluation of risk. Reducing outrage can include efforts to assess a risk properly and to bear the risk.

Outrage can be created or reduced by at least twelve different factors:

1. *Voluntary versus coercive.* Risk bearers are less likely to experience outrage when they expose themselves to a risk rather than having the risk thrust upon them.
2. *Natural versus industrial.* Risk bearers have less of an emotional reaction to natural risks, such as a tornado, than to risks created by other people, such as hazardous waste.
3. *Familiar versus unfamiliar.* Risk bearers perceive familiar things as less risky than unfamiliar things.
4. *Memorable versus not memorable.* Risk bearers rate the risk higher when it is linked to some memorable event than when it is a little known event. Bhopal is memorable, increasing the perception of risk for similar pesticide production facilities.
5. *Dreaded versus not dreaded.* Risk bearers rate risk higher when that risk is linked to a dreaded outcome such as cancer.
6. *Chronic versus catastrophic.* Risk bearers rate risks they face every day, such as driving, less seriously than catastrophic events, such as airplane crashes.
7. *Knowable versus unknowable.* Risk bearers fear the unknown more than the known. A new risk should generate more outrage than a well-known risk.
8. *Control versus not in control.* Risk bearers feel more secure when they have the ability to control or regulate the risk. Again, the idea of driving versus flying in a plane fits well. People can control the car when they are driving but not the plane when a pilot is doing the flying.
9. *Fair versus unfair.* Risk bearers experience greater outrage from a risk if they perceive their burden from the risk carries a greater price than that of other people.
10. *Morally irrelevant versus morally relevant.* Risk bearers experience greater outrage if the risk is linked to immoral actions such as cutting corners to make profits than if the risk is related to some moral good such as curing a disease.
11. *Trustworthy versus untrustworthy.* Risk bearers experience less outrage if they trust the experts involved in the risk communication effort than if they lack trust in those experts.

12. *Responsive versus unresponsive.* Risk bearers feel more outrage when the company responsible for the risk is unresponsive to their concerns.[1]

Risk communicators need to assess their risks for each of the twelve factors to determine how much outrage they are likely to face. But it is critical to assess the outrage to understand its exact level and what factors seem to be driving the outrage.

Clearly risk communicators cannot control all twelve of these outrage factors. However, trustworthiness, responsiveness, and control can be influenced through the risk communication process. Through honest interactions, risk communicators can build trust with community risk bearers. Risk communicators can show they are responsive by addressing risk bearer questions and concerns. Finally, crisis communicators can provide information that helps risk bearers understand what control they do have over a risk such as how to respond properly if a hazardous chemical were released.

Risk communicators must be sure to use nontechnical language. As in crisis communication, technical language serves only to confuse risk bearers or create the impression the company is trying to hide behind fancy words. Finally, making comparisons is a useful strategy in risk communication for helping people evaluate risk. In a risk comparison, a new or unfamiliar risk is compared to an old or familiar risk. This helps people to understand the severity of risk by placing it in a context they can understand. But the comparison must be accurate. For instance, comparing an involuntary risk to a voluntary risk is an ineffective comparison. People will recognize the difference, and these comparisons are more likely to create anger than understanding. An example is when risks from an industrial facility (involuntary) are compared to the risks from smoking (voluntary). An effective comparison will match risks that are similar to one another. An example of a similar risk comparison is comparing the health risks of a synthetic pesticide to those of natural pesticides present in many foods.

Analogies are a type of comparison that finds a similarity between two things that are somewhat dissimilar. Analogies can be used to explain common chemical concentrations used by scientists. When discussing hazardous chemicals, a risk communicator may use the phrase *parts per million*. A common analogy is that one part per million is equivalent to one drop of gasoline in an automobile's gas tank. This analogy uses something people are familiar with, gasoline in a gas tank, to explain an unfamiliar concept.

RISK COMMUNICATION AND THE NEWS MEDIA

The news media frequently work against risk communicators. News coverage of risk is very superficial and serves to generate outrage. The news media want ratings and readers. Drama attracts viewers, listeners, and readers. The news story tells people they are at risk but does not give specifics about the risk, such as hazard information. The news media concentrate on possibility rather than probability. Companies should not rely on the news media to handle their risk communication.

CONCLUSION

Many organizations have a legal mandate to engage in risk communication. Organizations may find themselves needing to increase or decrease stakeholders' evaluation of a risk. Risk communication is complicated by the emotional reactions it evokes from stakeholders who must be risk bearers. Risk communication is the most effective when risk communicators work to understand and to address the emotional reactions to risk.

See also Risk Management; Terrorism and Chemical Facilities; and Types of Risk.

NOTE

1. Peter M. Sandman, "Risk Communication: Facing Public Outrage," online at http://www.du.edu/~scbeckma/EPM4700/outrage.htm (accessed 27 Feb. 2007).

VULNERABILITY ASSESSMENT TEAM

Geary Sikich

Risk is a concern for any organization. Smart organizations seek to understand their risks. A critical component of risk is vulnerability: a weakness that can be exploited or develop into a problem situation. One of the various ways of measuring vulnerabilities is using vulnerability assessment teams. David Apgar, author of *Risk Intelligence: Learning to Manage What We Don't Know*, uses the term *risk intelligence* to describe organizational efforts to weigh risks effectively. Risk intelligence involves classifying, characterizing, and calculating threats; perceiving relationships; learning quickly; storing, retrieving, and acting upon relevant information; communicating effectively; and adjusting to new circumstances.[1]

Apgar distinguishes two types of risk: learnable risk and random risk. Learnable risks are nonfinancial and can be quantified. Random risks are primarily financial and difficult to define and to quantify. Vulnerability assessment teams face the challenge of trying to understand both types of risks. This entry considers what these teams do and the factors to consider when selecting vulnerability assessment teams.

WHAT VULNERABILITY ASSESSMENT TEAMS DO

In short, vulnerability assessment teams try to determine the various vulnerabilities an organization is likely to encounter. To fully understand vulnerability assessment teams, it is helpful to define the central concepts used in vulnerability assessment, including key terms, business impact analysis, and the integrated approach to assessment.

The key terms are *threat*, an expression of intent; *hazard*, the chance of being harmed; *risk*, the possibility of occurrence; *vulnerability*, weakness realized; *contingency*, expected actions; and *consequence*, unexpected results. These key concepts play a role in the business impact analysis (BIA), which determines how each negative event an organization may encounter will affect various business operations. The BIA tries to quantify the loss in terms of business interruptions (how long of a disruption) and the financial impact of the disruption.

Most organizations employ a business impact assessment as an initial step in planning. The matrix below summarizes the general types of events that the BIA may assess. Scan the list, add your own unique risks, and then grade the probability and impact as high, medium, or low, and the effect as long term or short term.

Important as this task is, planners rarely identify unexpected events or give them consideration, paying attention instead to what we know—actual events. But how can we be sure an organization is ready to address vulnerability assessment if we do not account for unexpected events? Events expose gaps in our knowledge. For example, the matrix above does not take into account changes in customer needs or wants. Until recently, few organizations even considered pandemic planning, something that is now becoming a focus point. But we still do not tie achieving corporate goals and objectives to the assessment of risks, threats, vulnerabilities, or hazards. Today's environment calls for a more robust review of vulnerabilities and risk.

The following example illustrates the effects of unexpected risks/overlooked vulnerabilities. Jeffrey R. Immelt, appointed chairman of the board and chief executive officer of General Electric on September 7, 2001, is the ninth chairman in GE's 128-year history. On September 12, 2001, Immelt was confronted with an unexpected event: "I was Chairman for two days. I had an airplane with my engines, hit a building I insured, was covered by a network I owned, and I still have to increase earnings by 11%."[2] Due to the chain of events that ensued, General Electric could not rely on the insurance operations or the jet engine division to deliver its contribution to the company's strategic earnings objective. Immelt had to turn to other divisions to increase their contributions in 2001. What may have been mission critical before the disaster was no longer so after September 11, 2001. The lesson is that planners must change their view of what's important after a disaster. Circumstances, customers, competitors, and investors—not its managers—define what is vital within a company after a disaster. Recognizing this fact and responding to it is imperative, if a company plans to achieve its strategic goals after a disaster.

Business Impact Assessment Matrix

Potential Events: Risks/Threats/ Hazards/Vulnerabilities	Probability (H, M, L)	Impact (H, M, L)	Effect (LT, ST)
Bomb Event			
Bomb Threat			
Customer Injury on Premises			
Data Entry Threat/Employee Error			
Disruption of Courier/Mail Delivery Service			
Earthquake			
Executive Succession			
Explosion			
Fire			
Fraud/Embezzlement			
Health Event (Employee Life Safety)			
Heating/Cooling Failure			
Hurricane			
Kidnapping/Extortion			
Lightning			
Loss of Critical Personnel			
Medical Event—Public Health Related			
Natural Gas Leak/Carbon Monoxide			
Pandemic			
Power Failure			
Robbery/Assault			
Severe Weather Conditions			
Snow/Ice			
Software Failure/Virus			
Tampering with Sensitive Data			
Telecommunications Failure			
Terrorist Act			
Tornado/Wind Damage			
Unauthorized Access/Vandalism			
Water Damage/Rain Storms			
Weapons of Mass Destruction (WMD)			
Weapons of Mass Disruption (Chem/Bio)			
Workplace Violence			
Additional vulnerabilities not listed here			

Notes: H = high, M = medium, L = low, LT = long term, ST = short term.

But common techniques used by vulnerability assessment teams fail to explore these random risks/overlooked vulnerabilities. (Refer to the BIA matrix for an illustration of the typical focus for risk and vulnerability assessments.) Under the last category, “Additional vulnerabilities not listed here,” an organization rarely accounts for external factors that relate to random risks and vulnerabilities such as changes in customer preferences as a recognized vulnerability. The point is the vulnerabilities and risk assessments are more complicated than traditional techniques used by most vulnerability assessment teams.

Traditional analysis is unable to predict all behavior in a dynamic environment. Therefore, adopt an integrated approach. One such is the *Active Analysis* methodology, developed by Logical Management Systems Corp. (LMS). LMS's methodology, based on the U.S. military's "Joint Special Operations Targeting and Mission Planning Procedures" (JP 3-05.5 10 August 1993), is termed *futureproofing*.

Futureproofing is an active analysis process that enhances decision making by identifying behavior patterns in a dynamic environment.[3] Active analysis can be subdivided into the following three categories of possible threats/occurrences (based in part on the work of Dr. Ian Mitroff[4]):

- *Natural threats/occurrences/consequences* consisting of such things as drought, floods, tornadoes, earthquakes, fires, and other naturally occurring phenomena
- *Normal threats/occurrences/consequences* consisting of such things as

  Economic disasters, such as:
    - Recessions
    - Stock market downturns
    - Rating agency downgrade, etc.

  Personnel disasters, such as:
    - Strikes
    - Workplace violence
    - Vandalism
    - Employee fraud, etc.

  Physical disasters, such as:
    - Industrial accidents
    - Supply chain disasters
    - Value chain disasters
    - Product failure
    - Fires
    - Environmental disasters
    - Health and safety

- *Abnormal threats/occurrences/consequences* consisting of

  Criminal disasters, such as:
    - Product tampering
    - Terrorism
    - Kidnapping and hostages, etc.

  Information disasters, such as:
    - Theft of proprietary information
    - Hacking, data tampering
    - Cyber attacks, etc.

Reputation disasters, such as:

- Rumors
- Regulatory issues
- Litigation
- Product liability
- Media investigations
- Internet reputation, etc.

Note that abnormal threats/occurrences/consequences are becoming more of the norm than abnormal, as we see the normalization of threats such as hacking and data tampering.

Think about each of these potential risks. How might these risks affect your operations? Profitability? Organizational structure? Industry prospects? Customers and vendors? This is futureproofing.

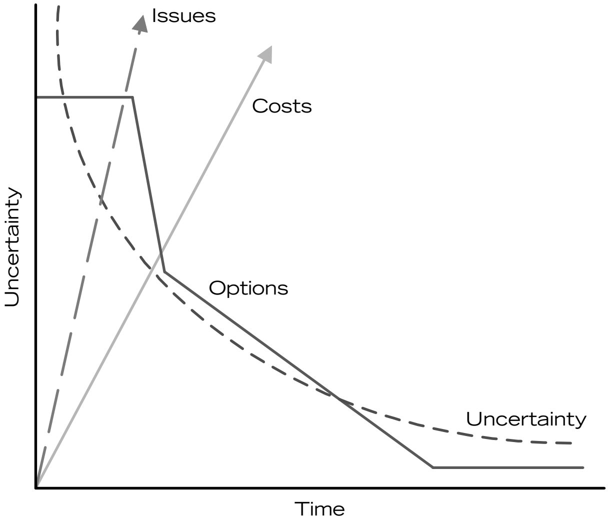
The following five key assumptions serve as a basis for developing the futureproofing framework:

- *Assumption 1.* The modern business organization represents a complex system operating within multiple networks.
- *Assumption 2.* There are many layers of complexity within an organization and its "value chain."
- *Assumption 3.* Due to complexity, active analysis of the potential consequences of disruptive events is critical.
- *Assumption 4.* Actions in response to disruptive events need to be coordinated.
- *Assumption 5.* Resources and skill sets are key issues.[5]

Based on the above assumptions and the results of the baseline analysis, one realizes that the timely identification, classification, communication and response, management, and recovery from a disruptive event are critical. As depicted in the graphic below, uncertainty decreases over time, as do available options for response and recovery. Increasing numbers of issues and higher and higher costs are also associated with response and recovery efforts over time. The more you can anticipate, the better for all.

The ability to effectively respond to and manage the consequences of an event in a timely manner ensures an organization's survivability in today's fast-paced business environment. With the emergence of new threats—such as cyber terrorism and bioterrorism—and the increasing exposure of companies to traditional threats—such as fraud, systems failure, fire, explosions, spills, and natural disasters—vulnerability assessment teams need a more effective, integrated approach to assessing business risks, threats, vulnerabilities, hazards, and the subsequent planning based on these analyses.

The vulnerability assessment team also must learn continuously about evolving and emerging risks, threats, vulnerabilities, hazards, and their potential consequences. Doing so facilitates their exposure early, before the full effects are



Graceful Degradation and Agile Restoration

really felt. An integrated approach overcomes the limitations of the traditional approaches described earlier.

Summary

The vulnerability assessment team needs to think beyond traditional ways of doing its job. These teams should employ an integrated approach that includes futureprooofing. Teams can then identify and prepare for a great range of risks and vulnerabilities, thereby producing a more complete vulnerability assessment and saving time and money in the long term.

CONSTRUCTING THE VULNERABILITY ASSESSMENT TEAM

Once we know what to assess, the challenge is to build the most effective assessment team. Creating this team involves two central concerns: (1) its composition and (2) its organization. A well-crafted team is more likely to be effective than one hastily put together. Too often, management forgets the need to develop teams thoughtfully.

To determine the composition of the assessment team, management should ask and answer a series of questions: What skills must the team possess? What level of experience? Who should lead the team? Whom does the team report its results to? Addressing all these questions helps in achieving a meaningful analysis of threats, vulnerabilities, risks, and hazards that allows the organization to implement actions that reduce or contain them.

Vulnerability assessment team members should possess a working knowledge of the organization's mission, goals, objectives, critical assets, policies, plans, and procedures. Team members need to include those who have passed a vulnerability assessment training course, understand physical and cyber security assessment processes, and are aware of business continuity planning principles. Others who may be appropriate to involve in this process are those with expertise in the various areas and issues associated with vulnerability assessments and emergency response/emergency response planning.

Given that the information on threats, vulnerabilities, risks, hazards, and consequences probably will come from sources external to the team, the team may wish to interact with other stakeholders. To that end, team leaders may choose to invite representatives from government, law enforcement, and emergency response planning communities to be part of the team on an ad hoc basis. Management must select a team that has the necessary skills, knowledge, and abilities to perform its required tasks.

Once the team is selected, the focus shifts to organizing concerns. The team should have six points of focus.

1. Strategy, or "What is the organization committed to?" This must be answered in two ways. First, you have to understand the organizational goals and objectives. Ask, "What are we in business to accomplish?" Also clarify the goals and objectives of the assessment, which can generally be identified on three levels: strategic, grand tactical, and tactical. As depicted in the table below, these three levels have common functions that must be understood at all levels within the enterprise.

	Strategic Assurance Level	Grand Tactical Continuity Level	Tactical Response Level
Executive Level			
Management Planning Operations Logistics Finance Administration External Relations	Support to continuity efforts Communicate outwards (stakeholders) Strategic active analysis		
Business Unit Level			
Management Planning Operations Logistics Finance Administration Infrastructure External Relations		Support to tactical level implementation efforts Sustain business operations Communicate upwards Grand tactical active analysis	

(Continued)

	Strategic Assurance Level	Grand Tactical Continuity Level	Tactical Response Level
Response Level			
Management Planning Operations Logistics Finance Administration Infrastructure External Relations			Direct specific response implementation steps Communicate upwards Direct mitigation efforts Tactical active analysis

2. Concept of operations, or “How will the organization meet its commitments?” Besides identifying vulnerabilities, determine how to mitigate the vulnerability or at least reduce exposure to the vulnerability.
3. Structure, or “Do we have an organization that serves our needs?” The assessment team must reflect a level of expertise appropriate to the scope of the assessment.
4. Resources, or “What are they and how are they going to be employed?” First and foremost, access the expertise and resources, including human resources, needed to get the job done. A network of knowledge is essential. Establish a learning repository for members of the team so they can exchange information and improve skills.
5. Core competencies, or “What skills do we expect from the vulnerability assessment team?” We must establish each team member’s knowledge as well as the degree of difficulty of learning about risks, threats, vulnerabilities, and so on. Learnable risks become less uncertain if we commit the time and resources to find out more about them. Random risks are such that no amount of analysis of causes or drivers can make them less uncertain. The team has to be able to identify and categorize the learnable and distinguish them from the random. Although information technology facilitates learning more about specific risks, threats, and so forth, depending on a single source can lead to “tunnel vision.”
6. Pragmatic leadership, or “How will we optimize authority, decision making, work flow, and information sharing?” The team leadership must ensure the appropriate sharing of information. Each vulnerability assessment team member needs to contribute to the assessment to help the enterprise achieve its goals and objectives.

A carefully constructed vulnerability assessment team is a valuable organizational asset. Team members are selected because they have the necessary knowledge, skills, and abilities to conduct the type of vulnerability assessment the organization requires. In short, the composition of the team reflects the nature of the vulnerability assessment tasks.

CONCLUSION: SEIZE THE INITIATIVE

A vulnerability assessment team with a broad base of expertise and experience enables changing some of the basic assumptions regarding how to measure risks, threats, and vulnerabilities. The learning organization gains a better picture of the implications of these identified risks and threats, and its ability to manage, mitigate, and/or minimize their potential effects is enhanced. Moreover, a vulnerability assessment team should utilize an integrated approach that includes futureproofing.

A Chinese proverb states that “Opportunity is always present in the midst of crisis.” Every crisis carries two elements: danger and opportunity. No matter the difficulty of the circumstances, no matter how dangerous the situation, at the heart of each crisis lays a tremendous opportunity. Great blessings await those who find the opportunity within the crisis.

Today business leaders protect their organizations by facilitating continuity planning and preparedness efforts. Using their status as leaders, senior management and board members can and must deliver the message that survivability depends on being able to find the opportunity within the crisis.

Many people believe that the world has changed as a result of the events of September 11, 2001, and that we need to rethink our concepts of continuity and crisis management. Today we cannot merely think about the plannable or plan for the unthinkable, but we must learn to think about the unplannable. Vulnerability assessment teams are a key part of planning and preparing for the unthinkable.

See also Business Continuity; and Risk Management.

NOTES

1. David Apgar, *Risk Intelligence: Learning to Manage What We Don’t Know* (Cambridge, MA: Harvard Business School Publishing, 2006).

2. Sahil K. Mahtani, “General Electric CEO Made Rapid Rise,” *The Harvard Crimson Online Edition*, online at http://www.thecrimson.com/printerfriendly.aspx?ref=508054 (accessed 23 April 2007).

3. Geary Sikich, “Futureproofing: The Process of Active Analysis,” online at http://www.idsemergencymanagement.com/Common/Paper/Paper_37/Geary%20W%20Sikish%202%20Active%20Analysis%20Futureproofing (accessed 23 April 2007).

4. Ian I. Mitroff, *Smart Thinking for Crazy Times: The Art of Solving the Right Problems* (San Francisco: Berett-Koehler Publishers, 1998).

TYPES OF RISK

Krista Varney

Businesses in general face many types of risk. This collection focuses on discussions of security-related risk, but other types should be considered as well. The same factors used to evaluate security risk can be applied to other forms of risk. Financial risk seems to be the most prevalent and well known, but businesses must address other types of risk in their day-to-day operations as well as in decision making. In addition to security and financial risks, organizations face legal, political, and operational risks. This entry looks at each type of risk and how it impacts an organization's sense of security.

FINANCIAL RISK

Financial risk is comprised of multiple areas of risk such as credit risk, interest rate risk, and market risk, to name just a few. Financial risk should be considered with any major investment decision. Here is an outline of each type of financial risk.

- Credit risk is simply the risk that a debt will not be repaid. Creditors evaluate the risk by looking at credit history and current financial position using various financial models. This type of risk is mitigated through interest charged on the loan and other provisions or covenants added to the loan agreement to protect the lender.
- Interest rate risk is related to changes in the level of interest rates or an interest rate relationship. For example, bond prices tend to fall as interest rates rise and vice versa. Investors can mitigate the risk through portfolio diversification, which is ensuring a mix of investments that help manage the impact of changes in interest rate levels. Hedging is another method used to mitigate interest rate risk by making another investment to reduce the risk of an existing investment.[1]
- Market risk is the risk that the value of an investment will change due to a change in the overall market. The most common factors that can cause a fluctuation in the market are changes in stock prices, interest rates, the value of foreign currency, and the value of commodities. Companies also typically mitigate market risk through investment diversification and hedging.

LEGAL RISK

Organizations also face risk that is not based on investments or lending. All companies are subject to legal risk, which is "uncertainty due to legal actions or uncertainty in the applicability or interpretation of contracts, laws or regulations."[2] One aspect is the risk that a company will be the plaintiff or defendant in a legal proceeding. Another is a precedent set by a ruling in a case that may indirectly affect the organization. Yet another is the risk that a new law or regulation will be put into place. The company may need to make changes to conform or be subject to fines or other penalties. Conforming to such requirements can be very costly and time consuming, so businesses must be diligent to stay current on the changing legal environment. Failure to comply can also be very expensive and detrimental.

POLITICAL RISK

Political risk is another area companies must evaluate, particularly those that operate internationally. Changes in leadership, civil unrest, and war may have an impact on a company's ability to operate. For example, a shift from a predominantly Republican to a Democratic Congress will likely affect the types of legislation that is proposed and passed. Just as with legal risk, companies must stay current on the political environment of every country in which they operate.

OPERATIONAL RISK

The risks of a shortage in the workforce or equipment breakdown are examples of operational risk that also may impact businesses. Any internal threat to a company's ability to perform its functions can be classified as operational risk. Companies may have little control over external risks such as legal and political risk, but they do have more control over operational risk. The threat of employees getting injured on the job can be mitigated through safe operating procedures, equipment inspections, and disability insurance. Threats to facilities from natural disasters can be mitigated by disaster recovery procedures and business continuity planning. Businesses must identify the potential threats to their operations and evaluate the controls in place to mitigate those risks.

CONCLUSION

Whether it is financial, legal, political, or operational in nature, organizations face risk in a variety of different areas. The key is to have a strategy in place to evaluate the changing risk landscape continuously and act accordingly to prevent loss. Understanding the various types of risk and applying best practices to mitigate the risk are good first steps in addressing them.

See also Risk Management; and Terrorism.

NOTES

[1] "Legal Risk," http://en.wikipedia.org/wiki/Risk (accessed 3 March 2007).
[2] "Risk," http://www.riskglossary.com/link/legal_risk.htm (accessed 3 March 2007).

CRISIS MANAGEMENT

W. Timothy Coombs

Business security and crisis management intersect in two important ways. First, a security problem can become a crisis that requires management. Second, business security functions are essential to many aspects of crisis management. The discussion of crisis management begins with a definition of terms followed by an explanation of the process and its relationship to security.

WHAT IS A CRISIS?

Before defining crisis management, first identify what constitutes a crisis. People use the term loosely. A person spilling coffee on a contract and a paper jamming in the fax machine are often called "crises." For companies, we need a higher standard of what constitutes a crisis versus an incident. A crisis is an unpredictable event that poses a significant threat that can harm an organization, industry, or stakeholders if handled improperly. Volcanologists study volcanoes. They know an active volcano can erupt but cannot predict when. Crises are much like volcanoes; a company expects one to occur but does not know when it will happen. Most crises are sudden, but some develop slowly as people neglect the warning signs.

A situation must pose a significant source of harm to be considered a crisis. Crisis expert Ian Mitroff cites the difference between incidents and crises. Incidents are small events that create limited, localized disruptions. An example would be someone burning popcorn in the microwave located in the company's vending area. It smells bad, but it is easy to "repair" the situation. If the popcorn were to spark a fire that required the evacuation of the building and caused serious damage, that would be a crisis. The evacuation would disrupt operations, result in a loss of revenue, and there could be some property damage from the fire.

Notice that the term *threat* is used with a crisis. We often think of a crisis as events producing actual harm, but a crisis can just be the potential to inflict negative effects. If proper action is taken, the negative effects can be prevented or limited. Negative effects come in many forms, including human injury or loss of life, financial loss, erosion of the company's reputation, structural or property damage, and environmental damage. Recalling a defective product before it harms consumers or containing a hazardous material spill to a small area is an example of preventing or reducing negative outcomes.

The negative effects can harm the organization, the industry, and/or stakeholders. Employee casualties, loss of reputation, structural or property damage, and financial loss are potential negative effects on an organization. A 2005 explosion at the West Pharmaceutical facility in Kinston, North Carolina, illustrates these effects. A total of six workers were killed, the facility was destroyed (structural/property), the company's safety questioned (reputation), and the production capacity decreased (financial). An industry can suffer loss of reputation and financial resources as well. An *E. coli* outbreak in spinach in 2006 was still being felt by the spinach industry in early 2007. Sales were down (financial) as people associated spinach with *E. coli* (reputation).

Stakeholders can suffer casualties, property damage, and financial loss. Two examples illustrate how crises threaten stakeholders. Say there is a large explosion and fire at a manufacturing facility. People near the facility could be injured by the shock of the blast or from flying glass caused by the explosion. The blast could damage nearby businesses and homes, while the fire could threaten those structures as well. Nearby businesses can lose money if they need to close for an evacuation or because roads leading to their facilities must be closed as part of the response to the explosion and fire. Or consider a toy oven for children that has a slight manufacturing defect. That defect could result in children being seriously burned by the toy (casualties) or igniting home fires (property damage and financial loss).[1]

WHAT IS CRISIS MANAGEMENT?

The purpose of crisis management is to prevent or lessen the negative effects of a crisis, thereby protecting organizations, industries, and stakeholders. Crisis management can be defined as a set of factors designed to combat crises and to lessen the actual damage inflicted by a crisis. The four basic factors in crisis management are prevention, preparation, performance, and learning.

Prevention encompasses the actions taken to avoid crises. *Mitigation* is another term used to indicate prevention. Prevention is based on identifying risk factors and warning signs. Any number of risks in an organization can become a crisis. Products, consumers, employees, and the manufacturing process are but a few examples. Refer to the Risk Management entry for further information on risks. One means of prevention is trying to reduce the risks. Consider an organization that uses a variety of hazardous materials in its production process. Any one of those chemicals could cause a crisis if it were released. Prevention/mitigation could involve replacing a hazardous chemical with a nonhazardous chemical that does the same job. Or smaller amounts of the hazardous chemical could be stored on-site to lessen the damage done if it were to be released. But a company cannot eliminate all risks. Some risks have no effective way to be reduced or eliminated, whereas others are cost prohibitive to reduce or eliminate. If risks exist, the potential for a crisis exists. Steven Fink, a pioneer in crisis management, argues that all crises have warning signs, which he calls prodromes.[2] One task for a crisis manager is to locate and take action on these warning signs. A series of small incidents during unloading of hazardous chemicals could indicate the potential for a crisis. Managers should act to improve the safety of the unloading process. Although crises may have warning signs, they are not always easy to see. As a result, crises remain a possibility.

Prevention assumes that the mitigation efforts will be effective. Management must evaluate the mitigation efforts to determine whether they can work and whether they are working. The first question is: "Will the prevention efforts produce results?" If the mitigation efforts have a low potential to succeed or will result in only a small magnitude or small change, management may choose not to attempt mitigation. The investment in mitigation must have the promise of actually producing results. If mitigation seems unlikely to yield results, management should continue to monitor the risk carefully for signs of an emerging crisis. If the mitigation efforts are employed, management needs to determine whether the desired level of risk reduction was achieved.

If we believe we cannot eliminate all risks or catch all warning signs, we must be prepared to respond to a crisis. Preparation is the most well known of the crisis management factors because it includes the crisis management plan (CMP), which provides guidance during a crisis but is not a detailed "how-to" document. Each crisis is unique and requires the crisis team to adapt as it addresses the crisis. The entry Crisis Management Plan provides additional information, and the Guidance Appendix offers a generic framework for a CMP. The crisis team is the other visible part of preparation. An organization designates a team that will be responsible for "managing" the crisis. The entry Crisis Management Team explains the composition and selection of this team. A critical element of preparation is training related to specific aspects of the crisis management process. Exercises are an important component of training, as they try to simulate a crisis. Refer to the entry Exercise and Training Basics for additional information on the subject.

Eventually an organization faces a real crisis and the team must perform. The performance factor requires the crisis team to apply its skills and knowledge to the crisis. The CMP serves as a guide, but the crisis team must be flexible and make critical decisions based often on limited information. Crisis performance is a very public event. Stakeholders are watching as the crisis might negatively affect them in some way. Do they need to evacuate? Did they eat at that taco restaurant? Do they have that brand of tires on their SUV? Crises are custom made for the news media, especially if there are dramatic visuals such as smoke or fire. Media coverage extends the potential number of stakeholders who will become aware of and monitor the crisis. The entries Crisis Spokesperson and

Crisis Management provide additional insights into communicating with stakeholders during a crisis.

The final crisis factor is learning. Once a crisis is over or an exercise completed, the crisis team should analyze how it and other people in the organization performed. Learning is not placing blame. The quickest way not to learn from a crisis is to try to blame individuals or teams for failure. The analysis tries to identify what worked so it can be retained and what did not work so a different and hopefully more effective strategy can be used next time. Ideally we learn and improve from exercises, but sometimes the real thing creates the learning opportunity. The two key points of the analysis are the crisis management plan and the crisis team. The analysis should determine whether the CMP was effective or ineffective. Did it provide useful information for the team, or was it missing information the team needed? You want to find the holes in the plan and fill them. The crisis team needs to be evaluated to determine whether the team composition is working. Was there a critical functional area of the organization that was not but should have been on the team? Did any individual team members have problems handling their duties? Great employees do not always translate into great crisis team members. The stress of crisis can break some people. The entry Crisis Management Team discusses this point in greater detail.[3]

THE STAGES OF A CRISIS

Steven Fink was among the first to describe crises as having phases. Each phase creates unique demands for the crisis managers and involves different crisis management factors. Crises have three phases: precrisis, crisis, and postcrisis. The precrisis phase involves those actions taken before a crisis ever occurs. Prevention and preparation are the key crisis factors during the precrisis phase. Prevention or mitigation shows the connection between crisis management and emergency management. Refer to the Benefits of Emergency Management entry for more information on the mitigation topic. The crisis team needs to monitor its environment by actively scanning the known sources of crisis risk to see whether there are any signs a crisis is developing. This includes but is not limited to accident reports, safety evaluations, regulatory violations, and attempts to breach the computer system. A crisis sensing mechanism is used to collect and funnel relevant information to the crisis team or crisis manager. Refer to the Crisis Sensing Mechanism entry for a more detailed discussion of this crisis management tool.

Preparation involves the development of the CMP, the hiring of a crisis manager, and the creation and training of a crisis management team. An organization should have at least one individual dedicated to crisis management to assure that someone is held accountable for regular crisis management activities. An organization can consider making crisis management a part of the annual evaluation of the other crisis team members as well.[4]

The crisis stage is when a crisis hits and an organization must respond with a combination of operational actions and communication actions. Operational actions that address the crisis could include deployment of fire suppression, chemical containment, evacuations, shelter-in-place, activation of a hot site, or recall of a product. The crisis management team must coordinate with the business continuity team, which decides what actions are necessary to keep the organization operating, including the use of a hot site. It is important that the two teams coordinate on business continuity issues to prevent a duplication of efforts. Refer to the Business Continuity entry for more information on this topic. Operational actions are decisions made by the crisis team, which must use communication to collect the information required to make these decisions. Crisis teams rarely have all the information they need, but some data must be collected and analyzed before operational decisions can be made. For instance, because it is expensive to activate a hot site, the team must have a solid reason for making that choice.

Security personnel are vital during a crisis response. A member of security should be part of the crisis team to provide a security perspective on decisions. Security guards/officers are often a crucial part of the crisis team's eyes and ears during a crisis. They are usually the first ones to the crisis site and can provide real-time information as to what is happening. Security guards/officers can also coordinate with first responders and help track the number of injuries as well facilitate any evacuations or shelter-in-place orders. If a hot site or other temporary facility is used, security guards/officers must make sure that facility meets its security requirements.

The crisis team needs to communicate with various stakeholders including employees, community members, government agencies, the news media, investors, and supply chain partners. A good example would be a fire and explosion at a chemical processing facility. Employees must be told to evacuate, when they will report back to work, and how pay will be handled during the crisis. Nearby community members must be notified whether they need to evacuate or to shelter-in-place. The relevant government officials must be alerted. The news media will want information about what has happened and how the company is managing the situation. Investors should be briefed on the potential financial impact of the crisis. Supply chain partners include your suppliers and your customers. Suppliers need to know whether they need to make deliveries, make adjustments to the amount delivered, or deliver to your hot site. Customers must know whether there will be deliveries and the size of those deliveries. The entries Crisis Communication: External and Internal and Crisis Management supply additional information about communication during a crisis.[5]

During the postcrisis phase, efforts to manage the crisis are winding down and an organization is returning to business as usual. Admittedly it can be fuzzy as to when a crisis is moving from the crisis to the postcrisis phase. The defining characteristic is that the crisis has become a low priority and operations seem to be back to normal. A number of lingering crisis concerns still must be addressed but do not preoccupy or consume the organization. The focus of postcrisis is the transition to normal operations, follow-up communication, and the learning crisis management function.

An organization needs to transition from its business continuity efforts to normal operations. This could mean returning to a facility from a hot site or other temporary location after the damage has been repaired or the facility rebuilt. Security guards/officers must be ready for this transition as well by making sure the reopened facility is properly secured.

Follow-up communication includes updates on progress to recover from the crisis, actions taken to prevent a repeat of the crisis, delivery of information promised to stakeholders during the crisis, release of reports about the investigation of the crisis, and providing information to any governmental agencies that are investigating the crisis. Part of follow-up communication is making sure that employees, supply chain partners, and investors are up-to-date on efforts to return to normal operations. Suppliers and customers need to be informed exactly when the supply chain will be fully restored. Suppliers must know where shipments go when there is any shift in location from a hot site or temporary location back to the original facility. Investors require updates on the projected financial impact of the crisis.

People who suffered losses from the crisis (the victims) need to know the steps the organization has taken to prevent a repeat of the crisis and the progress of any claims they may have filed for restitution. For instance, a company may reimburse community members for expenses during an evacuation or pay for repair work such as new windows or cleanup. During the crisis the crisis team may not know the answer to all the questions it receives but promises to provide that information once it is known. The organization builds credibility by delivering on all of its promises in the postcrisis stage.

No matter what type of crisis occurs, some investigation of the cause will occur. The higher the news media profile of the crisis, the more intense the interest in the investigation will be. The investigations vary in the degree of formality and the parties involved. Some are conducted by government agencies such as OSHA or the U.S. Chemical Safety Board, whereas others are managed by the organization itself. The organization must cooperate by supplying the necessary information to governmental investigations. For high media profile crises, an organization wants to release the finding of its own report. Examples of the public release of internal reports for high media profile crises include E. F. Hutton and its check kiting scandal in the 1980s, Mitsubishi and its sexual harassment epidemic in the 1990s, and BP and its Texas City explosion in 2005. Government reports can draw media coverage as well for high media profile cases. BP and its Texas City explosion in 2005 also exemplify this. The media reported extensively on the Chemical Safety Board's 2007 report on the Texas City explosion. Organizational reports can include the corrective actions being taken, thereby addressing the prevention concerns of victims. Follow-up communication must be accomplished in a timely manner and be clear to the target audience. It can be a challenge to translate technical information from an investigation into understandable information for stakeholders.

The final element of the postcrisis stage is learning, which is executed after the crisis is "over." It can be done while follow-up is occurring but the bulk of the crisis has passed. Learning can be accomplished with exercises as well, so exercises are included in this discussion. It is ideal to learn from exercises so that mistakes do not become translated into actual casualties and other losses. Learning involves dissecting exercises and actual crises to determine what worked and what needs improvement. Other names for the dissecting process include *debriefs* and *postmortems*, with *postmortem* being the favored term.

Postmortems focus on the effectiveness of the crisis management plan, performance of the crisis management team, and performance of organizational employees. An exercise or crisis helps to determine whether there are any holes in a CMP. Was critical contact information missing or wrong? Should some additional information be added to or deleted from the plan? Similarly, the postmortem reviews the performance of all those involved in responding to the crisis such as the crisis team and any other employees who played a part in the crisis management effort. The focus is on the crisis team. Did people understand and were they able to perform their roles? Did particular members have trouble coping with the stress? You also want to determine whether other employees knew and followed the proper procedures such as evacuations or shelter-in-place.

A postmortem collects data from a variety of sources including the records kept during the crisis or exercise, observations made during an exercise, interviews with those involved, and surveys of people involved with the crisis management effort (including community members if they were affected). Surveys can ask crisis team members to evaluate specific performance aspects of other team members and their assessment of the CMP.

Communication is a critical part of the crisis management process, so it is a key component of a postmortem as well. This can be as simple as discovering whether the CMP contact information is useful and as complex as determining the effectiveness of disseminating the various crisis messages to the many stakeholders involved in the crisis management effort. Employees can be surveyed to determine their reactions to the parts of the crisis management process that affected them and their suggestions for points that could be improved. For instance, how effective was the employee notification system? Was it timely and accurate? The Crisis Learning box contains additional sample questions for a postmortem that can be used for both crisis team members and those not on the team.

Learning is used to improve the entire crisis management process. Some experts recommend dividing the analysis by crisis management functions or by crisis activities so the organization can better understand what specific elements of the crisis management process need work or are strengths. The postmortem can reveal a risk or threat that had not been high on the organization's list or even on its crisis radar. Exercises and crises can uncover CMP flaws or identify weak crisis team members. A postmortem can lead to a CMP being revised or a crisis

Crisis Learning Postcrisis Evaluation Survey Tool

Sample introductory statement: At _________, we are constantly trying to improve our crisis management performance. Improvement requires a thorough review of our crisis management efforts. Your feedback is an important part of the evaluation. Please provide honest and complete answers to the following questions. If you wish, your answers will be anonymous; just skip the optional information section. Thank for your time and help with our evaluation process.

OPTIONAL INFORMATION

Name: Phone:

Department/Organization:

SAMPLE SURVEY ITEMS/INTERVIEW QUESTIONS

What role did you play in the crisis management process?

How did you learn about the crisis?

Were you satisfied with the crisis notification system?
Why or why not?

How would you rate your unit's crisis management performance?

1	2	3	4	5
Very Poor	Poor	Average	Good	Excellent

How would you rate the organization's overall crisis management performance?

1	2	3	4	5
Very Poor	Poor	Average	Good	Excellent

Were you asked to supply information to the crisis team?
Was the request understandable?
Why or why not?

Was the request reasonable?
Why or why not?

What other suggestions do you have for improving the crisis management process?

SAMPLE SURVEY ITEMS/QUESTIONS FOR CRISIS TEAM MEMBERS ONLY

Were you satisfied with the process the team used to collect information?
Why or why not?

(continued)

Were you satisfied with how other organizational units responded to the team's information requests?
Why or why not?

Were you satisfied with how external stakeholders responded to the team's information requests?
Why or why not?

Which units/stakeholders were especially helpful?

Which units/stakeholders were especially problematic?[7]

team member being replaced. The improved preparation should translate into more effective responses when a crisis hits.[6]

Many organizations hire vendors to run simulations for them. While expensive, vendors add a number of advantages. First, the crisis team does not have to spend time developing the crisis exercise; the vendor will customize one for the organization. Second, vendors can provide very realistic scenarios and create the feel of a crisis. And third, vendors can supply a postmortem of the crisis management effort. This third point might be the most important. Learning can create a defensive climate. A vendor provides an objective set of trained eyes rather than peer evaluations from people with limited crisis experience. Also a team might have trouble being self-evaluative. An organization does not have this luxury of vendor evaluations when learning from an actual crisis.

A postmortem is based on information collected from people involved in the crisis management effort. If the crisis management effort went poorly, this can create a barrier. People might view a postmortem as a search for scapegoat and, as a result, may be reluctant to provide pieces of negative information. In general, evidence shows that people do not like to disclose bad news in an organization, especially if it reflects negatively upon them. The challenge to effective learning is to create a climate in which people know the purpose of the postmortem is to improve the crisis response and not to try to pin blame on anyone. Advice on how to specifically address such a challenge is beyond the scope of this entry. However, management should recognize that learning from a crisis does present certain challenges.

WHY THE CONCERN ABOUT CRISIS MANAGEMENT?

This entry on Crisis Management is rather long. What justifies devoting so much attention to crisis management? The answer is that organizations' demand for effective crisis management keeps increasing rather than decreasing. An organization does not have crises all the time, but scanning the news media any day will uncover any number of crises ranging from product harm to fires to chemical releases to explosions. A crisis can happen at any time, and there are five reasons why organizations are under pressure to develop effective crisis response measures: stakeholder activism, the value of the organization's reputation, negligent failure to plan, a broader view of crises, and communication technologies.

Stakeholders are those groups or individuals that can affect or be affected by an organization. Key stakeholders include customers, investors, employees, the news media, the community, and activist groups. When stakeholders are angry at an organization, they can make it harder for that organization to operate. One term for this effect is *stakeholder churn*. Angry stakeholders can exact a penalty on organizations by creating a crisis. Crisis experts agree that angry stakeholders are now in a very strong position to create a crisis for an organization. Angry stakeholders want an organization to change; that need for change is a crisis. Stakeholders are challenging that the organization is acting inappropriately, and if others share this view, a crisis develops.

One reason for increased stakeholder activism is that the Internet provides a forum for reaching other disgruntled stakeholders. Through the use of web sites, blogs, and discussion boards, stakeholders can reach out to others. These technologies are known as consumer generated media (CGM) or social media. People create the messages and can connect with one another through these various media. There is strength in numbers. The more stakeholders who believe an organization has done wrong and is in crisis, the stronger the crisis. Why stronger? CGM and social media are forms of word of mouth. Negative word of mouth hurts an organization. The Kryptonite bicycle lock case is an excellent example of the power of negative word of mouth and the Internet. Kryptonite makes popular high-end locks for bicycles. Owners of the lock began posting information to the Internet that many versions of the lock could be picked by simply using the outer casing of a Bic pen. People even posted videos showing how it could be done when they perceived a slow response from the company. Their goal was to pressure Kryptonite into recalling the lock. The activist consumers were perceived as having won when Kryptonite agreed to their demands. It appeared as though Kryptonite was forced into making the recall and design changes.

Moreover, the disgruntled stakeholders may attract traditional news media attention resulting in negative publicity for an organization, damaging its reputation. Boycotts are an excellent example. Boycotts do not succeed on an economic level, but organizations give in to them because of the negative publicity. Burger King and Wendy's agreed to a demand from the People for the Ethical Treatment of Animals (PETA) to sign a declaration involving buying animals slaughtered humanely. It was not the economic impact of PETA members not eating at Burger King and Wendy's that won the day. Rather the Murder King and Wicked Wendy web sites and news media coverage of the protest created the change.

An organization's reputation is how its stakeholders evaluate it. Is it being viewed favorably or unfavorably? Refer to the entry on Reputation Management for more details about what a reputation is and how it is formed. Business leaders once questioned the value of a reputation, but that is no longer the case. Now there is consensus among experts in business that a reputation is a valued asset for an organization. A favorable reputation attracts benefits and an unfavorable one creates problems. A crisis is a threat to an organization's reputation because it places the organization in a poor light. The organization becomes associated with a bad event (the crisis) that may or may not be of its own doing. Stakeholders make that connection and the organization's reputation suffers. How management reacts to the crisis helps to determine how much damage a crisis can inflict on its reputation. Outstanding responses can even lead to an organization improving its reputation. Consider how after twenty years, Johnson & Johnson is still praised for its handling of the first Tylenol poisoning crisis. Ineffective crisis responses can intensify the damage to the organization's reputation. Exxon, now Exxon-Mobil, is still haunted by the *Valdez* accident and oil spill. The entry Crisis Management explains how crisis managers can try to protect reputations during a crisis. A crisis places an organization's reputation at risk, and effective crisis management is one way to protect a reputation from harm.

Negligent failure to plan is not a new concept to people involved in business security. Organizations have long been held accountable if they did not take reasonable actions to reduce or eliminate known or reasonably foreseeable risks that could result in harm. The original intent was to protect employees. The 1970 Occupational Safety and Health Act established that organizations could be held liable for not providing adequate safeguards. Part of risk management is designed to eliminate reasons for negligent failure to plan lawsuits. Over the past few years, the scope of negligent failure to plan has expanded in the workplace. The risks now include workplace violence (see the entry Workplace Violence Prevention and Policies), product tampering, terrorism, and industrial accidents. All four of those events can be considered crises. See the entry Types of Crises for additional details. An organization can be held legally liable if it does not (1) take actions to prevent these crises and (2) prepare to respond to these crises. So, there are legal reasons to engage in crisis prevention and preparation. Both can serve as a defense against negligent failure to plan. Juries are already awarding damages to plaintiffs and punishing organizations that have not engaged in proper crisis management. The term *due diligence* comes to mind. Crisis management is now a form of due diligence because it provides evidence that management has taken action to avoid harm to others and the organization. Engaging in accepted crisis management practices can serve as legal defense in some lawsuits spawned by a crisis.

A broader view of crisis refers to how crisis managers have expanded their views of crises after the 9/11 attacks. Prior to the 9/11 attacks, few organizations included terrorism attacks in their crisis planning. As noted earlier, terrorism is now a part of negligent planning so there is an expectation that crisis management efforts will include terrorism targets. Physical security has been an essential feature in efforts to prevent terrorist activities. Refer to the entries

Terrorism and Physical Security for more information on the subject. But what if your organization is not a prime target, such as a transportation center, historic area, government operation, or chemical facility? Your organization may be near a target and be affected by those attacks. Crisis managers now have a greater awareness of collateral damage from other organizations' crises. A terror attack could result in road closures, evacuations, or shelter-in-place orders that will affect your organization. Chemical, biological, or radiological terror attacks could affect a very wide area.

Communication technology was mentioned in the discussion of stakeholder activism. The Internet and the various communication tools available through it can be used to create a crisis. An entire industry has developed around monitoring the Internet for warning signs of a crisis. Combine the Internet with twenty-four-hour news networks, and the world is a small place. Organizations can no longer believe that actions in distant places will stay hidden from view. Either CNN or some Internet message can reveal these once hidden acts. Consider Coca-Cola having to deal with pressure from U.S. college campuses about worker abuses in South America. The abuses were made public through news stories and the Internet. College students agitated successfully and advocated for change (having colleges drop contracts with Coca-Cola) using materials from the Killer Coke web site. Organizational actions are becoming much more visible, thanks to communication technology.[7]

CONCLUSION

Crisis management must be integrated into an organization to be effective.[8] Such integration should include interfacing with security on issues related to prevention, preparation, and action. In addition, crisis management must coordinate with related areas of business continuity, emergency preparedness, and disaster recovery to avoid duplication of actions and promote smoother implementation of the response to a crisis.

See also Business Continuity; Crisis Communication: External and Internal; Crisis Management; Crisis Management Plan; Crisis Management Team; Crisis Sensing Mechanism; Crisis Spokesperson; Benefits of Emergency Management; Physical Security; Risk Management; Types of Crises; and Workplace Violence Prevention and Policies.

NOTES

1. W. Timothy Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, 2nd ed. (Thousand Oaks, CA: Sage, 2007), pp. 2–4.

2. Steven Fink, Crisis Management: Planning for the Inevitable (New York: American Management Association, 1986), 15–18.

3. Coombs, *Ongoing Crisis Communication*, pp. 5—6, 17–20.
4. Coombs, *Ongoing Crisis Communication*, pp. 21–61.
5. Coombs, *Ongoing Crisis Communication*, pp. 127–149.
6. Coombs, *Ongoing Crisis Communication*, pp. 151–163.
7. Coombs, *Ongoing Crisis Communication*, pp. 7–11.
8. W. Timothy Coombs, *Code Red in the Boardroom: Crisis Management as Organizational DNA* (Westport, CT: Praeger, 2006), pp.107–109.

TYPES OF CRISES

W. Timothy Coombs

Among the first tasks of a crisis team is to brainstorm a comprehensive list of crises that the organization could encounter. This list will be very long and vary according to an organization's industry and geographic location. Different industries and geographic areas have diverse risks that can develop into crises. Crisis experts recommend that organizations create a crisis portfolio instead of trying to develop responses to a massive list of crises. A crisis portfolio groups similar crises together. The crisis team then prioritizes the crises and constructs the crisis management plans around the portfolio. Refer to the Crisis Management Plan entry for information on crisis prioritization. Generally, crises fall into one of three categories: (1) attacks on an organization, (2) when things go wrong, and (3) misbehavior by members of the organization. Each of these crisis types presents unique challenges and opportunities for crisis managers.

ATTACKS ON AN ORGANIZATION

Organizations can be victims of crises. Outsiders or insiders can attack an organization. Attacks are premeditated actions intended to harm the organization and/or its personnel. Attacks can create collateral damage on stakeholders as well. When an attacker poisoned Tylenol capsules with cyanide in 1982, customers died. These deaths overshadowed the financial losses of its manufacturer Johnson & Johnson. Such attacks' focus is primarily to seek to damage a reputation or to inflict financial loss (including destroying data) but may involve property damage and casualties among employees and/or stakeholders. Attacks on an organization include product tampering, workplace violence, terrorism, computer hacking/tampering, and rumors. A number of the entries in this volume relate to attacks on an organization, including Agroterrorism and Ecoterrorism. Clearly security is an important factor in attacks on an organization.

The current dependency on computers and the Internet creates a significant vulnerability for organizations. Computer hacking/tampering is meant to cover the wide range of attacks that can be thrown at an organization's computer system. This can include denial of service, compromised data, damaged or deleted data, or defacing of web sites. Denial of service is a risk for organizations that use their web sites to conduct business. This can include sales or investing. A denial of service is rather easy to execute. You can even download programs from the Internet to facilitate a denial of service effort. The basic process is that the web site becomes overloaded with traffic causing the web site to "crash." The traffic prevents legitimate users from accessing and using the web site. In February 2000, a denial of service attack hit a number of web sites including Amazon.com and eBay, resulting in financial losses in excess of $100 million. Information security is an important resource in defending an organization against computer hacking/tampering.

Cyber attacks can come from the inside as well as the outside. The U.S. Department of Homeland Security finds most inside attacks are employees trying to exact revenge on a boss. Insiders have easy access to computer systems and can cripple networks, damage data, or delete critical software. In March 2002, the U.S. offices of an international financial services company were hit with a logic bomb. A logic bomb is a form of malicious code that is embedded in a system and timed to activate at a later data. The logic bomb affected over 1,300 servers and destroyed 10 billion files, for an estimated financial loss of $3 million. The logic bomb was planted by an employee unhappy with his annual bonus. Refer to the entry Insider Threat for additional information on this topic.

Regardless of the nature of the attack, computer hacking/tampering causes financial loss and can damage the organization's reputation as well. Attempts to attack computer systems are common. Accurate statistics are difficult to find, however. The FBI believes only about 34 percent of all attacks are reported because companies fear negative publicity. Because of this secrecy, a number of states have passed laws mandating that companies tell individuals, mostly customers and employees, when their personal data may have been compromised. The best way to prevent and to detect computer hacking/tampering is through effective information security. Organizations must install and update firewalls and other security software. Employees need to know and follow cyber security policies. The computer system must be monitored for attacks as well. The Information Security entry provides greater detail on prevention.

Rumors are untrue information about your organization that is publicly circulating. In most cases, that incorrect information is harmful to your organization's reputation and/or its bottom line. The Internet has made it rather easy to spread rumors through e-mails, blogs, and postings to discussion groups. An excellent example of a rumor is Febreze, a fabric refresher that eliminates odors. The original version was a spray. If there is an odor on fabric, spray on Febreze. The advertising focused on smoke and pet odors. Shortly after Febreze was introduced, people began receiving e-mails saying it could kill or harm dogs and cats. The information was untrue and threatened sales. A key target audience was given a strong reason not to buy the product. Procter & Gamble, the maker of

Febreze, responded quickly. It dedicated a section of its web site to debunking the rumor. The site contains testimonials from veterinarian associations and the American Society for the Prevention of Cruelty to Animals (ASPCA) supporting the safety of Febreze and links to their web sites for additional information.

Management must decide whether the rumor is really a threat. The threat posed by a rumor is a function of how believable it is—does it seem plausible?—and how widespread it is. If a rumor appears in multiple places online and in the news media, it is a threat. If the rumor is one or two people on seldom read blogs, it is not much of a threat. Organizations must fight rumors that are threats. When rumors appear online, the organization needs to post replies online. Use the same discussion boards where the rumor appears, and dedicate space on your own web site to disprove the rumor. Disprove the rumor with the facts and support of others, just as Procter & Gamble did in the Febreze case. Rumors do not go away if you ignore them. They can have a long life span, even in cyberspace. Rumors cannot really be prevented but can be detected. Part of an organization's monitoring of the Internet should include rumors about it or its products. Refer to the entry Crisis Sensing Mechanism for additional information on monitoring the Internet.

Product tampering occurs when an individual or group alters a product to cause harm or for its own financial gain through extortion or fraudulent lawsuits. Consumers are at risk with product tampering. People have died from tampered versions of Sudafed and Tylenol. Most people remember when the woman found a fingertip in her Wendy's chili. The management of Wendy's remembers because of the financial and reputation loss from the incident. Police were able to prove the case was product tampering; the woman had placed the fingertip in her own chili so that she could sue Wendy's. The fingertip came from a coworker of her husband who had accidentally cut it off at work. Part of the investigation was an autopsy on the fingertip, which found the finger had not been cooked so it entered the chili very late in the process and raised a red flag for tampering. This meant the fingertip did not enter during the product's trip through the supply chain.

Every day we encounter products with tamper-resistant packaging and products we consume in some way. Consumable products are the prime targets for tampering. The entry Agroterrorism presents additional information about tampering. It is the injury or threat of injury that can inflict financial damage, be a reason to pay the extortion, or offer grounds for a fraudulent lawsuit. Packaging is the key preventative. People should not consume products when the tamper-resistant measures are no longer intact. Is the plastic ring on the bottle broken or the cover on the peanut butter torn? Still, a skilled attacker can find means to tamper with a product without compromising the seals.

An organization confronted with a product tampering case must investigate the claim. Security can be essential to the investigation. In addition, the organization's safety measures can be used as part of the evidence to prove it was tampering. The investigation should determine whether the tampering claim is a hoax designed to extort money or there has been some contamination of a product. A hoax is treated like a rumor by proving it does not exist. If there is real contamination, the product must be recalled before it does harm or further harm. Security can help to oversee the proper disposal of the recalled products.

Workplace violence, a growing concern in the United States, involves someone in the workplace becoming a victim of a violent act. The violence may be perpetrated by a random customer, another employee, and a former employee, or by someone else the person knows, such as an enraged spouse. The most shocking type of workplace violence is employee on employee. The news media love to cover stories about employees or former employees lashing out in the workplace. The Nu-Wood Decorative Mill in Goshen, Indiana, made the national news when an employee shot and killed one coworker and wounded six others. Workplace violence occurs in all types of work settings from blue collar to white collar and large urban areas to small towns. Refer to the entries on Workplace Violence Prevention and Policies, Workplace Aggression, and Contributors to Workplace Aggression for extended discussions of this topic. The focus here is on workplace violence as a crisis. When an organization responds, the focus must be on the victims, not the organization. Management must express concern for the victims and their families along with explaining how it intends to help them, such as by covering medical costs or supplying psychological counseling.

Terrorism involves the use of violence or threat of violence against people or property to create fear or intimidation to achieve some objective. Product tampering and terrorism are closely linked. Extreme activist groups can use tampering or threats of tampering to pursue their political agendas. Refer to the entry Ecoterrorism for more information on extreme activist groups and terrorism. The Terrorism entry details the risks and ways to prevent terrorist attacks. In responding to a terrorist crisis, the organization must warn stakeholders about any threats. What danger does the terrorist incident present to community members, employees, or customers? Stakeholders must be warned and told what they should do to protect themselves from harm. Also report any actions the organization is taking to aid victims of the attack. After the warnings are supplied, the focus shifts to business recovery. The organization needs to communicate its timeline for return to normal operations to its stakeholders.

Attacks on an Organization Case Studies

ChoicePoint: Compromised Data

ChoicePoint is a data brokering firm providing information that businesses and government agencies use to verify information about people. Its data are used for identification and credential

(continued)

verification that help its clients detect fraud and reduce risks. ChoicePoint's own web site notes how protecting privacy is a priority. How ironic that ChoicePoint lost sensitive data for about 145,000 people in a pseudo-hack. In March 2005, ChoicePoint began notifying people that their identities could be at risk due to a security breach characterized as a "hack." California law required this disclosure. It is estimated that the security breach cost ChoicePoint $15 million to $20 million.

Many in the information security field claimed this was not a hack and that ChoicePoint had sold the information to a bogus client. One man has been arrested and charged in the crime. The thieves used fax machines at a Kinko's office to run the scam. This was fraud, not a hack. Later, ChoicePoint's own chief information security officer, Rich Baich, claimed the incident was unrelated to information security, so it was not his responsibility. Again, people in the information security field took exception. The position was that the actions were malicious activities designed to misuse or inappropriately obtain data, so it was information security. Information security has a larger scope than protecting computer systems from attacks. Information security is not limited to just the technical aspects of information; it also must seek to prevent data from being compromised against a variety of malicious activities. Following the event, ChoicePoint launched an extensive effort to strengthen the verification of its clients. These actions included creating an independent office to oversee client credentialing and partnering with Ernst & Young to develop an industry-leading compliance program.

Lockheed Martin: Workplace Violence

On July 8, 2003, 911 calls were reporting shootings at the Lockheed Martin facility in Meridian, Mississippi. Employee Doug Williams shot and killed six coworkers and wounded eight others before killing himself. One of those wounded died a week later. Management stated it was "shocked and saddened by this tragedy and express our deepest sympathies to the families."

Strangely, Doug Williams began that workday in a mandatory ethics and diversity training session and stormed out of the training after just a few minutes. As he left, Williams confronted his supervisor, Jeff McWilliams. McWilliams claimed Williams was angry and said he would take matters into his own hands. Williams

(continued)

exited the building, went to his pickup truck, and returned with a shotgun, a rifle, and ammunition. He began shooting people in the training room and then killed two more people at their workstations before killing himself.

Later reports shed new light on the shootings. All but one of the victims was African-American. Williams was a known racist. A year and a half before the shootings, Williams had been reprimanded for making racist comments and death threats to African-American coworkers. Those killed in the shootings included the coworkers believed to have made the complaints. This case shows how a crisis can change. The Lockheed Martin shootings were beginning to look like management misconduct. Lockheed Martin did not follow its zero tolerance policy for death threats. Williams should have been fired for his comments but instead was sent to anger management classes. There is now a lawsuit pending against Lockheed Martin because of management's failure to act on the warning signs of workplace violence.

Pom Wonderful: Product Tampering and Terrorism

Pom Wonderful markets a variety of healthy fruit juices. Its flagship product is Pom Wonderful Pomegranate Juice. Pom Wonderful claims its juices work by negating free radicals, a substance linked to various diseases. The science Pom Wonderful uses comes from research laboratories, some of which experiment on animals. The People for the Ethical Treatment of Animals (PETA) and other animal rights groups have denounced Pom Wonderful for this practice.

One of those other groups was the Animal Rights Militia, a radical animal rights group. In December 2005, the Animal Rights Militia announced on its web site and to the news media that it had tampered with Pom Wonderful Pomegranate Juice in East Coast grocery stores. It claimed to have laced the drinks with chemicals that would cause rapid bowel fluctuations, fatigue, and vomiting. Some stores did pull the product. Pom Wonderful began testing its products, found no tampered products, and denounced the incident as a hoax. Pom Wonderful's news release on the subject referred to the hoax as a terror tactic, an accurate categorization. Product tampering was being used to create fear, inflict harm on the organization, and promote a political agenda. Pom Wonderful has since announced it will no longer be involved in product testing on animals.

WHEN THINGS GO WRONG: ACCIDENTS

Bad things happen even to good organizations. That is part of the mantra that no organization is immune from a crisis. You can follow all the safety protocols, have the best safety training, and carefully inspect all products, but accidents can happen and products can malfunction. Safety and quality will never be 100 percent. A part wears out in a toaster resulting in a fire hazard three years after purchase; a piece of equipment is mislabeled by the manufacturer and breaks when used to unload chlorine; or children are injured from the misuse of a toy. All of these things have happened and will happen again. Sometimes things just go wrong.

Crises when things go wrong are accidental in nature. The organization did not purposefully have an accident or ship a defective or dangerous product. The company did not intend and/or could not control the circumstances that resulted from the crisis. The organization was taking steps to prevent crises but things happened. The six types of accidental crises are (1) technical error product harm, (2) technical error industrial accidents, (3) transportation mishaps, (4) loss of key personnel, (5) challenges, and (6) unpopular decisions.

Product harm is when a product an organization makes can hurt consumers in some way. Technical error means the product harm was a result of unforeseen circumstances. People in the organization did not know harm would occur because the danger was undetectable through normal procedures. The Taco Bell *E. coli* poisoning and Dell laptop battery fires are classic examples. Taco Bell employees had no way of knowing that the lettuce they were using was contaminated with *E. coli*. Dell and other manufacturers did not know the batteries they were using had particles inside that could cause them to overheat and potentially catch fire. Typical product harm events include contaminated foods, mislabeled foods (not disclosing all ingredients), and defective mechanical parts.

The accidental nature of technical error product harm makes it difficult to prevent. The best preventive measures do not work all the time. Organizations need to constantly monitor customer complaints for signs of a pattern that may indicate product harm. Are a number of similar problems, illnesses, or injuries being reported? If so, work with government agencies to determine whether the situation warrants a recall of your product. If a recall is necessary, follow the procedures outlined by the federal government. Copies of these can be found in the Guidance Appendix. It is also important to express concern for those adversely affected by your product. Management may want to offer covering all the medical costs for those injured by the product. Paying for the medical costs helps to reduce the anger felt by the victims and lessens the likelihood of a lawsuit.

Technical error industrial accidents refer to situations in which the cause was beyond the reasonable control of a person or the organization. An individual would have difficulty detecting the risk that led to the accident. Fires, explosions, and chemical releases are common forms of industrial accidents. Granted, all accidents have a mix of technical and human causes. A technical error industrial accident implies the primary cause or causes were technical rather than human error. In January 2003, the West Pharmaceuticals Rouse Road facility was destroyed by an explosion that killed six employees. The facility made syringe plungers and intravenous fitments. The cause of the deadly explosion was organic dust; rubber dust, to be more precise. Organic dust has the potential to ignite and to explode. Rubber dust had collected unseen in a suspended ceiling, and some ignition source reached the dust and destroyed the building. There are no government regulations about rubber dust or any other organic dust except in grain elevators. The West Pharmaceuticals tragedy resulted in the U.S. Chemical Safety Board issuing new warnings about organic dusts.

Again, the nature of technical error industrial accidents makes them difficult to prevent. Organizations should carefully read new warnings from government officials about risks that are not covered by government regulations. The response should follow a pattern similar to technical error product harm. Employees and those living near the facility need to be told how the crisis will affect them and what they might need to do to protect themselves, such as evacuate the area. Management should express concern for the victims and provide aid if that seems prudent.

The final technical error crisis is the transportation mishap, an accident that kills or injures people because a vehicle did not perform as expected. Buses and trucks should stay on the road, trains should stay on the tracks, and planes should take off and land safely. It is a technical error mishap when the primary cause was not controllable by those involved in the crisis. Airline transportation mishaps draw the most attention because of their dramatic nature.

TWA Flight 800 best exemplifies the technical error transportation mishap. On July 17, 1996, TWA Flight 800 left New York for Paris. Not long after takeoff, the Boeing 747 exploded over the Atlantic Ocean. There were no survivors; all 230 people on board perished. The news media conveyed a constant stream of stories, and networks broadcast live from near the water's edge. The National Transportation Safety Board (NTSB) spent $36 million over four years to investigate the crash. Its conclusion was that some electrical charge caused the center fuel tank to explode. The NTSB recommended inspecting the wiring on a number of different types of Boeing aircraft after the tragic mishap. No other Boeing plane before or since has exploded in this way. It was a problem that was not known and would not have been found during regular maintenance. It took a crisis to bring this technical error to light.

Prevention of technical error transportation mishaps is a matter of learning. The organization learns from its mishaps or those of other organizations. This new risk is now factored into preventative efforts. Transportation mishaps typically require a system for notifying next of kin. For large-scale accidents, organizations need to deploy trauma response units for victims, the families of victims, and employees. Focus your response on concern for the victims and what the organization is doing to help the victims and to find the cause of the crisis.

Top leadership is an important influence on many investment decisions, especially the chief executive officer (CEO). A CEO can shape share price and impact the organization's overall reputation. The sudden loss of a leader can be a threat to an organization, whether it is the result of an unexpected death, a serious illness, or a decision to leave the organization. Whatever the cause, the loss of key management personnel can be considered to be a crisis.

In April 2004, Jim Cantalupo, the CEO of McDonald's, was preparing to address a meeting of owner/operators in Orlando, Florida. The event was designed to celebrate Jim's success in increasing profits at McDonald's. Before he could give his presentation, Jim suffered a heart attack in his hotel room. He died later in a hospital at the age of sixty. It was a stunning loss that could have been problematic for McDonald's. Fortunately the organization had a succession plan and had its next CEO, Charlie Bell, already in a senior management position, which meant the company could move quickly and effectively to fill the leadership void. You cannot prevent people from dying suddenly or from leaving a company. An organization must have a succession plan that is kept current and draft executive contracts that specify a certain amount of notice before leaving to prevent unexpected exits. In the case of death, the organization must first honor the fallen leader, which puts a human face on the organization and its loss. The next step is the same regardless of the reason for the vacancy: fill it quickly with a quality person. The smoother the succession is, the less the disruption and threat. A quick transition reassures stakeholders that the organization is in safe hands.

Challenges are a unique crisis type. They occur when a group accuses the organization of acting improperly or unethically. It is not that the organization has done anything illegal; the group disagrees with what an organization does or how it does it. Recent examples include buying fish from Iceland, policies extending health benefits to same-sex partners, and buying chickens that were not raised in a humane manner. Management must decide whether the challenge is a legitimate threat to its reputation. The question is, "Will other stakeholders support this challenge and see the company as acting inappropriately?" Challenges can generate negative publicity and promote negative word of mouth on the Internet.

People for the Ethical Treatment of Animals (PETA) uses a combination of publicity stunts, usually involving celebrities, and Internet messages to pressure companies such as McDonald's, Burger King, and Wendy's. Companies negotiate with PETA if they fear the negative publicity and that the Internet messages could hurt their reputations. In June 2001, PETA launched a campaign to have Wendy's agree to an animal welfare program. McDonald's and Burger King had already agreed to follow the guidelines. The effort was known as the Wicked Wendy's campaign. A web site for Wicked Wendy's showed a red haired girl with a bloody knife and contained information that documented Wendy's noncompliance with the guidelines. Actor James Cromwell helped to draw attention by being arrested with five others at a protest in a Vienna, Virginia, Wendy's.

Following the publicity stunt, Wendy's management began negotiating with PETA, and an agreement was reached in September 2001.

Challenges can be effective and organizations must be prepared to evaluate and respond to them. Not all challenges are reasonable, and an organization should defend its decision to stay the course of action. The Walden book chain refused to give into pressure to remove a list of "unacceptable" books from its stores. Management viewed the challenge as censorship. Security can help by making sure any protests at the organization's facility are peaceful and that the organization's response is measured. Overreacting to protestors only makes the media coverage worse.

The final variation of when things go wrong is an unpopular decision. There are times business reasons dictate that management execute tough measures such as layoffs and plant closings. Stakeholders may disagree with the actions and protest against them. The unpopular policies are not illegal but can result in some damage to an organization's reputation. The crisis is self-inflicted to a degree. But if the business situation dictates drastic measures, management must do what it can to protect itself and its core stakeholders. The idea is that management had little control over the decision. Of course, the element of control may be disputed by those angered by the actions. Management must make sure it can provide evidence to support that the actions are a sound business choice given the current economic situation.

When Things Go Wrong Case Studies

Chic-Chi's: Technical Error Product Harm

Chi-Chi's used to be a chain of Mexican restaurants. A common ingredient in many of its dishes was green onions. The green onion is the main reason Chi-Chi's is no longer in operation. By 2003, Chi-Chi's was already under Chapter 11 bankruptcy protection. The restaurant chain was having some difficulties but was trying to rebound. That effort came to halt in the fall of 2003 when reports began to link Chi-Chi's to a hepatitis outbreak centered in Pennsylvania. The incidence was traced to a Chi-Chi's restaurant in the Beaver Valley Mall about twenty-five miles northwest of Pittsburgh.

The outbreak was very serious. Three people died and 640 others were sickened. The state of Pennsylvania provided hepatitis vaccine to people who thought they might have been exposed. The initial fear was that an infected worker had passed the disease on to the customers. The Food and Drug Administration (FDA) proved the

(continued)

cause of the outbreak was the green onions, not any workers. The workers had been exposed to the disease just as the customers had, through the green onions. The FDA noted that Chi-Chi's was a victim in this case. Chi-Chi's personnel had no way of telling the green onions were infected. There were no actions the workers could have or should have taken to prevent the hepatitis outbreak because the disease was undetectable under normal circumstances. No restaurant is required nor expected to test all incoming food products for potential disease. Customers were slow to return to Chi-Chi's and the chain went out of business.

American Family Association (AFA) and Ford: Challenge Crisis

The American Family Association (AFA) is a conservative Christian organization created and operated by minister Donald Wildmon. Its goal is to protect traditional family values. The AFA concentrates on cleaning up television and other media. It seeks to remove antifamily content and promote profamily content. The AFA targets companies that advertise on television shows that the AFA believes attack traditional family values. A common tactic is to pressure companies to stop advertising on an offensive show.

The AFA does take action beyond the entertainment industry when it fears traditional family values are under attack. One attack it sees is the support for a homosexual agenda. The AFA targeted Ford Motor Company for its support of the homosexual agenda/attack on traditional family values. The AFA is unhappy with Ford's support of homosexuals in the workplace and funding of homosexual organizations. The AFA is disturbed that the groups supported by Ford include those pushing for gay marriage rights. This goes against the AFA's defense of marriage platform. The AFA is asking people to boycott buying from Ford until Ford renounces its prohomosexual agenda. The boycott, first announced in the summer of 2005, was then postponed until 2006 to give the AFA and Ford dealerships time to negotiate. The boycott remains in operation through 2007 at the BoycottFord.Com web site.

Ford Motor views the inclusion of gays as part of its antidiscrimination policy. Ford does provide benefits for same-sex partners and does recruit employees on gay-oriented employment web sites. Ford management has repeatedly defended these actions. Ford does support gay organizations by funding events and buying advertisements in gay publications. The rationale is that Ford sees

(continued)

the gay community as one of its target consumer groups. Many other companies are tapping into the gay market as well. Although Ford management did talk with the AFA, Ford eventually decided to maintain its support for gay organizations and events through donations and advertising. Initially Ford management announced it would end advertising in gay publications but then reversed that decision. Ford management decided its commitment to diversity and targeting gay consumers was more important than the boycott by the AFA.

Sharp Electronics: Technical-Error Product Harm

In April 2005, Sharp Electronics announced a recall of approximately 370,000 Sharp 27-inch conventional tube televisions, including models 27RS50, 27RS100, and CSR5027. The sets were sold between March 2001 and February 2005.

The harm was a result of two factors. First, the power button could break as a result of simple use, leaving a hole at the front of the television set. The part was intended to be much more durable. Second, foreign objects could be placed through the whole. Reports indicated that straws, crayons, and metal objects had been put in the holes and created fire hazards. Sharp received twenty-three reports of fires. There were no reported injuries and a few reports of minor property damage. One fire was reported to have resulted in over $20,000 in property damage. Consumers were told to unplug the sets immediately and contact Sharp about a free repair.

Sharp did not intend for the power button to break and create a fire hazard. The television sets had passed safety inspections and were in working order. The power button simply failed to perform as intended. It took a number of years for the problem to surface. Some of the sets had been in homes for almost four years. The recall was technical and not a result of human error.

WHEN ORGANIZATIONS MISBEHAVE: MANAGEMENT MISCONDUCT

The worst possible crisis to manage is one that management makes for itself: management misconduct. The name Enron comes to mind. Enron executives used an elaborate and illegal accounting system to convince investors and employees that the company was making huge profits when it was not. There was no question of intention; management intentionally placed stakeholders at risk or violated legal or regulatory statutes. There are three variations of management misconduct: (1) known risk, (2) improper job performance, and (3) legal or regulatory violations.

Businesspeople have been known to place profits ahead of all else. Consumers can be in a dangerous situation when an organization knowingly places them at risk by selling products it knows to be dangerous in some way. A well-known example is the Ford Pinto, Ford's effort to compete with the Volkswagen. The goal was to keep the car under 2,000 pounds in weight and $2,000 in cost. Ford's own rear-end collision tested revealed a flaw. The fuel system easily ruptured, creating a fire hazard in rear-end collisions. The assembly line had already been set up when the flaw was discovered. Management rejected the two fixes presented by engineers as too expensive. Ford management compared the estimated cost of the repairs to the estimated cost of lawsuits from deaths and injuries. The lawsuit cost placed at $49.5 million was lower than the repair cost of $137 million. Ford sold Pintos knowing they were flawed and dangerous. In the end, the actual lawsuits cost Ford well over $137 million. Customers need some degree of trust in a company. Knowingly placing consumers at risk quickly erodes any trust.

People will make mistakes, including employees. While these errors may not be intentional, people hold organizations responsible when a crisis results from employee (human) error. People are not very sympathetic and believe that effective organizations should have eliminated the mistakes through proper training and supervision. Management is responsible because it did not provide proper oversight. Employee mistakes can be deadly or just embarrassing. In January 2003, an Air Midwest flight from Charlotte, North Carolina, crashed killing all nineteen people on board. The primary reason for the crash was improper maintenance. The Raytheon employees hired to maintain the aircraft had improperly adjusted the plane's elevation control. The investigation also found poor on-the-job training and supervision of the maintenance crews.

In the spring of 2005, a newspaper investigation uncovered an offensive in-house training video used by the San Francisco 49ers. The purpose of the video was to teach football players how to handle the news media is a high-diversity city. In reality the video used a number of racial stereotypes and slurs. The team was embarrassed and fired Kirk Reynolds, the man responsible for the video. Management knew the video existed and was being used but did not stop its use by the team. Such cases illustrate why people hold management responsible when employees fail to do their jobs properly.

Managers sometimes engage in illegal activities. They knowingly violate laws or regulations, often for their own gain. This includes abusing power through discriminatory or harassing actions. The illegal activities can result in financial loss and personal injury. Investors and employees lost millions of dollars due to the deception of Enron's top management. Mitsubishi had a case of widespread sexual harassment at one of its facilities. Management and even line workers regularly harassed female employees through groping, obscene gestures, and displays of pornographic images. Mitsubishi hired former Labor

Secretary Lynn Martin to investigate. Her report criticized how management had allowed the harassment to continue and to take an ugly toll on many of the female employees. Management knew the problem existed but did not seek to protect the workers.

Management misconduct can be difficult to detect because managers are in a position to cover up the actions. Many organizations now have ethics officers. Part of their job is to ferret out such illegal actions. Refer to the entries Ethics as a Business Security Concern and Ethica Conduct Audit for additional information. Some person or group needs to watch the watchers if management misconduct is to be discovered early and corrected before becoming a major media event. A public scandal adds damage to the organization's reputation in addition to any fines or legal consequences from the misconduct.

Organizations must be prepared to pay a steep price for management misconduct. In extreme cases such as Enron it can end an organization. People are very angry when management misconduct is revealed, so an organization must make a strong response built around accepting rather than dodging responsibility. Management must be prepared to take responsibility for the situation, express concern for the victims, enact changes designed to prevent a repeat of the problem, and make restitution to the injured parties.

Management Misconduct Case Studies

Cadbury Schweppes: Known Risk

Cadbury Schweppes is the world's largest confectionary company producing such well-known brands as Trident, Halls, Dr Pepper, Snapple, Cadbury, Schweppes, and Dentyne. In June 2006, Cadbury Schweppes recalled over 1 million chocolate bars including the Dairy Milk Turkish 250 g, Dairy Milk Caramel, Dairy Milk Mint bars, Dairy Milk 8 chunk, Dairy Milk 1 kg bar, Dairy Milk Buttons Easter Egg 105 g, and the 10 p Freddo bar. The recall cost Cadbury Schweppes over $58 million. The chocolate was contaminated with salmonella, the source being a leaky water pipe in its Marlbrook facility.

The recall was in June even though Cadbury Schweppes had discovered the problem in January 2006. Between January and June is Easter, the biggest sales time of the year. Some critics speculate that Cadbury Schweppes purposefully did not recall before Easter to protect its sales. Cadbury Schweppes management claimed the amount of salmonella was within allowable limits.

(continued)

The British government responded that there is no such thing as an allowable limit for salmonella. Any amount is cause for concern and a recall.

In total, thirty cases of salmonella were traced to the chocolate, according to Britain's Health Protection Agency. Cadbury Schweppes faces charges under British law for producing food unfit for human consumption. Cadbury Schweppes likely suffered additional revenue losses as a result of the damage this misconduct crisis inflicted on its reputation.

Tyco: Illegal Activities

If it were not for Enron, Tyco might be the name people think of for corporate greed and illegal activity. Led by one-time CEO Dennis Kozlowski, a number of Tyco's top executives illegally took over $600 million in cash and stock from the company. The money was obtained by abusing their positions to misuse Tyco compensation programs including relocation payments, automatic bonuses, and an employee loan program. Kozlowski helped to hide these illegal activities from the company's board of directors and told lower-level managers the actions were board approved. His lie to the lower-level managers kept them from reporting the activities to the board.

Kozlowski was the king of corporate excess and greed. He threw a lavish birthday party for his wife in Sardinia featuring actors playing statues and an ice sculpture of David that urinated vodka. The price tag was over $1 million, and Kozlowski used Tyco funds to cover the cost. In June 2005, Kozlowski and others were convicted in state court for misappropriation of funds and sentenced to jail time in September 2005.

Tyco investors paid a heavy price for this management misconduct. The stock price plummeted as the investment community lost faith in the once respected company. As in any management misconduct, there was significant damage to the company's reputation as well. Tyco has systematically been rebuilding its reputation and share price. Under the leadership of new CEO Edward Breen, Tyco has stressed its commitment to management integrity and ethics. This has included bringing in a corporate governance expert to reshape Tyco's practices and make management at all levels more accountable. Tyco has been developing a system it believes will make it easier to detect

(continued)

management misconduct and, hence, make management less inclined to engage in illegal and unethical behaviors.

BP at Texas City: Improper Job Performance

On March 23, 2005, a series of explosions ripped through the BP refinery at Texas City, Texas. In total, 15 workers were killed and 170 were injured. It was one of the worst industrial accidents in the United States since 1989. The explosion occurred when employees were restarting the hydrocarbon isomerization unit. The accident has been investigated by BP, by an independent commission established by BP, and by the U.S. Chemical Safety Board. The findings of the three completed studies and preliminary reports from the federal government all agree the accident could have been avoided. Its main cause was improper job performance.

Restarting the hydrocarbon isomerization unit is a dangerous process. Employees have admitted to violating the safety policies for the restart. One employee turned off an alarm that would warn when the unit was overfilling. Employees would violate the restart and overfill the unit so that the restart could be executed in a shorter amount of time. A manager trained in the process is to oversee the restart. The manager left during the restart process to attend to his son who had been injured at school, so no experienced manager was on duty when the explosion occurred at around 1:20 p.m. There were technical causes for the tragedy as well. BP was using the old-style, less effective blow stacks as a safety mechanism for the hydrocarbon isomerization unit rather than the more current and more effective flare system. It had been recommended that BP switch to a flare system, but this was not mandated by the government. Internal documents suggested BP did not make safety upgrades and was lax in safety training due to cutbacks designed to save money. Some management at Texas City had recognized the safety problems and asked corporate for help in improving safety, but no action had been taken until after the Texas City explosion.

Thus far, all evidence suggests the Texas City explosion was preventable. Had employees done their jobs properly, those fifteen lives would not have been lost. BP has set aside $1.6 billion to settle the lawsuits from the victims and their families. In early

(continued)

2007, BP settled one of the last major claims and has thus far avoided going to trial. The financial losses and damage to BP's reputation were of its own doing. Had BP maintained safety training and enforced safety regulations, the crisis probably would not have occurred.

CONCLUSION

Crises can be organized into three broad groups: attacks on organizations, when things go wrong, and misbehavior by members of an organization. Business security can help in detecting and preventing attacks on organizations and misbehaviors by members of an organization. Things going wrong are difficult to prevent, but security can be a valuable resource in the response. Organizations must be prepared to scan for and to face a variety of crises. This entry provides a framework for organizing the potential crises an organization might encounter.

See also Agroterrorism; Contributors of Workplace Aggression; Crisis Management; Crisis Management Plan; Crisis Sensing Mechanism; Ecoterrorism; Ethica Conduct Audit; Ethics as a Business Security Concern; Information Security; Insider Threat; Reputation Management; Terrorism; Workplace Aggression; and Workplace Violence Prevention and Policies.

NOTE

1. W. Timothy Coombs, *Code Red in the Boardroom: Crisis Management as Organizational DNA* (Westport, CT: Praeger, 2006), pp. 13–64.

CRISIS COMMUNICATIONS: EXTERNAL AND INTERNAL

Ágnes Huff

A crisis is an unexpected and potentially damaging event or situation that can have far-reaching negative consequences. Crises can come in many forms: a natural or technological disaster, financial or legal business crisis, or human-caused trauma such as workplace violence. All crises require timely and effective communication to facilitate essential information dissemination and create important first impressions. When employed properly, communications can help protect an organization's reputation.

The cornerstone of crisis response is coordinated communications with external and internal audiences. How an organization responds publicly to a crisis in the first few hours can have a significant and lasting impact on the organization's brand image, future business, and ultimately its long-term survivability. Changing public and media perception is a difficult process and best accomplished by an ongoing communications program.

As part of the overall response effort, communication plans provide for a systematic approach to disseminate key information during a real or perceived crisis. The goal is to be able to implement the tested strategies quickly and efficiently to communicate with the organization's key publics. External communication targets a broad range of constituencies including media, customers, shareholders, vendors, contractors, government officials, and the public. Internal communication, which is equally important, involves informing people within the organization, such as executives, employees, staff, and families.

A well-developed plan ensures a communication response is rapid, providing available information even when details are scarce. Serving as a blueprint for the most important tasks and activities an organization must undertake in a crisis, communication plans ensure that policy and procedural decisions do not have to be made in the midst of the chaos. Corporate accountability demonstrated through forthright communication can help an organization return to normal operations with minimal impact on its reputation.

Issues addressed in the planning phase facilitate a more coordinated and rapid response, demonstrating that the organization is in control, which instills public and employee confidence in the overall response. Scrambling at the onset of a crisis to find a spokesperson or attempting to contact employees with an outdated telephone list immediately creates a negative perception. Lack of crisis preparation often has a spillover effect that impacts business operations, reputation, and employee morale.

The communication plan must be reflective of the organization's beliefs, attitudes, priorities, and commitments. Just saying the right thing is being done is not enough, nor is it credible. An organization must be able to demonstrate and reinforce its core values and business ethics clearly by the actions it takes. This is especially true in crisis situations that involve ethics or executive misconduct; the public is growing increasingly more intolerant of lies, denials, and avoidance tactics and holds companies and their executives accountable.

Crisis communications is a high-stakes activity. When faced with a major, potentially devastating event, the primary goal of an organization is to emerge with its reputation and business intact. Values govern behavior, and the goal of communicating in a crisis is to convey the facts and crisis details within the context of the organization's values and business ethics. In order to do this, organizations must plan in advance, communicate rapidly, and do so with confidence.

THE TWENTY-FOUR-HOUR NEWS CYCLE

With rapidly expanding communications outlets, organizations cannot hide. Breaches of security, shootings, accidents, and natural disasters are reported within minutes of occurring. Citizen journalism, social media, cameras and videophones, YouTube, blogging, and the Internet's global reach offer the ability to spread information and misinformation at lightning speed. Traditional media's leadership role has been usurped by this technological convergence. An involved social citizen network now provides voluntary on-scene and timely coverage of breaking news and systematically engages them in commentary and dialogue.

When a crisis occurs, self-purported experts and others with an agenda are eager to be interviewed, voice criticisms, or assign blame before any facts are available. The job of the media is to fill the information void that is greatest immediately following a crisis. In lieu of facts, the news bottle can get filled by clues, accusations, and speculation. A proactive and prepared organization should anticipate this and make every effort to communicate the known facts, corporate background, and holding statements, leaving less room for speculation.

The news cycle is getting increasingly more compressed, requiring speed and transparency. Broadcast interview sound bites have been reduced to just five seconds from thirty. More information needs to be communicated more concisely and in less time. Being articulate, relevant, and engaging are essential attributes for communicators today. Information needs are immediate, often leaving little to no time for preparation. A communications delay, for any reason, is perceived as negative and can potentially cause financial loss, reputation damage, and severe impact for an organization.

CRISIS COMMUNICATIONS TEAM

Identification of the crisis communications team—who the members are and what roles they will play—is one of the first steps in the planning process. A competent and cohesive team will be able to instill confidence in an organization's response to a crisis, rather than cause damage to its reputation.

Decision makers need to be identified and a crisis chain of command should be established, which will eliminate conflicts of authority in a stressful crisis situation. Then, individuals with appropriate skills can be enlisted as members of the communications team. This does not always mean selecting the highest-ranking executives, but those who have demonstrated an aptitude for effective communications.

A crisis communications team must be tailored to each organization but may include some or all of the following team members:

- *Top executive*. The CEO/senior executive may make the initial statement communicating corporate responsibility and regret if an accident occurs that results in injuries, loss of life or property, or significant damage to the surrounding community. In serious crises, swift executive visibility can affect how the public perceives the company and its actions.

- *PR director.* The public relations or media relations director is in the best position with his or her credibility as the communicator and established media relationships. The media relations director's job depends heavily on the information from the crisis responders and the other members of the communications team to ensure that information is up to date and accurate.
- *Operational or facility manager.* In the case of an accident that impacts normal business operations, an operational manager is in the best position to provide information on details, developments, and local response actions. This individual can effectively serve as a link between operational response and public communication.
- *Legal advisers*. In this litigious environment, frontline communicators need legal guidance to minimize potential liabilities. On occasion, the objectives of crisis communicators to disseminate information may be at odds with attorneys who want to protect the company. These issues should be addressed in the planning phase.
- *Human resources*. Internal employee communications is generally handled by the human resources (HR) director, including workforce updates, notification of next of kin (in the case of injuries or fatalities), and potential workplace trauma. Human factors in crisis situations cannot be overlooked, and the HR role is responsible for communicating information internally to staff, debriefing, organizing employee assistance counseling, and other crisis-related personnel matters.
- *Finance director*. A finance director or insurance representative provides for emergency funds, ensures there is necessary communications equipment, and helps the communications representative support that the organization is prepared and poised to handle the crisis operationally, financially, and publicly.
- *Technical experts*. Media are increasingly more knowledgeable even with highly technical and specialized issues within an industry. Such technical expertise should be utilized to communicate factual and accurate information appropriately. Experts can include engineers, architects, professors, doctors, psychologists, union representatives, accountants, and others.
- *Independent third-party allies*. An often overlooked practice is the identification of credible third-party experts or allies, who can provide a relatively objective perspective, corroborate details, or reinforce the organization's preparation and training.

Critical Functions

Developing checklists for essential actions for each communication team member provides the foundation for a coordinated response, eliminating duplication of effort or confusion, both of which waste precious time and resources in a crisis.

Everything that can be done in advance to prepare for a crisis streamlines the communication process. Draft statements or press updates can be prepared and pre-approved, a crisis update page on the web site can be ready to mobilize, corporate background information can be available, distribution and crisis monitoring resources can be identified, communications equipment vendors can be on standby, and lists should be available to facilitate mobilizing support personnel to help field incoming inquiries.

By nature, crises are complex and dynamic, leaving only a small window of opportunity to do the right thing. Serious consequences can occur if communication is mishandled. Having identified and prepared a communications team in advance is one of the most important steps organizations can take to manage a crisis effectively.

MEDIA SPOKESPERSON

As the public face of an organization in a crisis, designated spokespersons have to be carefully selected. Serving as the voice of values and facts for an organization in crisis, these spokespersons need to be forthright, credible, accessible, and properly trained. First on the front line, they must gather and verify information quickly, translate responses into key messages, as well as evaluate the dynamic media climate to determine the best communication strategy. A spokesperson can help minimize potential damage to an organization's reputation and create a positive first impression, or can make a crisis situation worse.

MESSAGE MANAGEMENT

Crisis communications involves crafting thorough and compelling statements, known as "messages." It is essential to develop appropriate messages and anticipate tough questions that may be asked. The process of developing key information that should be communicated forms the foundation for both external and internal communications. Although messaging is generally tailored to each audience based on its informational needs, some essential elements of messaging should be addressed in virtually all crisis communications.

The necessary elements of external and internal messaging include the following:

- *Acknowledge the crisis*. To be credible, the obvious cannot be denied. If an accident has occurred, acknowledge it. This does not mean assume blame or accept liability; it means offering the facts about what happened.
- *Respond appropriately*. If there has been loss of life, focus on the human element first. Communicate compassionately and appropriately for the crisis situation. Cooperation, swift action, assistance to the victims, and doing the

right thing are all elements of appropriate response. Don't minimize or exaggerate the issues; just state the facts.
- *Move forward*. Get past the crisis quickly by communicating what is being done and what steps are being taken to prevent a reoccurrence. If there was an operational or procedural breakdown, explain the process to review the situation and revise procedures, or what immediate steps are being taken to address the situation.

MESSAGE DELIVERY

Once specific messages have been established for external and internal audiences, the challenge becomes how best to deliver the messages to ensure that they are received as intended. Communicators refer to this focused delivery of information as staying "on message" and not letting stress or pressure from the target audience get the communications off track. It involves a technique of creative repetition and reinforcement of the message.

After determining what should be said, the communicator must ensure that the language properly reflects the messages with carefully chosen words. In crisis communications response, using a human-centered vocabulary can ensure that the communicator comes across as a genuine and caring individual, rather than the face of a cold organization.

If the primary goal in a crisis is to communicate that the organization is prepared and responding appropriately, key messages can include the following:

- "Our corporate crisis plan was implemented immediately."
- "Rescue efforts are underway and we are cooperating fully."
- "We have trained professionals to notify families of the victims."
- "We are working to return to normal operations."

In handling questions, it is useful to restate and reiterate the key messages with every answer. All briefings for media, employees, or the public should always reinforce the key messages and end with a concise summary. Audiences tend to remember what is said at the beginning and end of a briefing, and it is important to leave them with the necessary information so they can form an appropriate perception.

The benefit of developing messages and draft statements in advance is to save time and allow the communicator to focus on more pressing priorities.

MEDIA MONITORING

Media monitoring plays a vital role during all stages of a crisis. On an ongoing basis, key search-term monitoring with Google or Yahoo! (e.g., name of the organization or issue) can return ongoing results for regular review and analysis, and signal trends, new competition, or regulatory involvement. A wide range of business audiences and influencers rely on the Internet for breaking news and information.

During a crisis, monitoring the media and public reaction is essential to guiding the communications response. Insight gained from media monitoring allows an organization to adjust its communications to better meet the needs of its constituencies. Monitoring alerts responders to crisis escalations, emerging issues, misperceptions, timing, and frequency issues and provides vital feedback on how messages are being received.

Organizations must obtain intelligence on what is being reported, who is publishing it, what bloggers are saying, what articles are linked, and even what speculation and misinformation are being republished. By knowing how information is being interpreted—and what allies and competitors are saying—communications can be targeted more effectively.

INTERNAL AUDIENCES AND SPECIAL NEEDS

Crisis communication for internal audiences is as important as it is for external audiences. Employees are key stakeholders who have direct contact with the company's external stakeholders. Even those who are not directly involved on the crisis response team need to receive accurate and up-to-date information to engender trust, confidence, and loyalty in their employer. In a business in which operations continue despite the crisis, employees on the front line who may also be affected must be prepared to handle crisis-related questions and queries from customers. They need to be briefed on their responsibilities, scope of authority, and how to respond to questions or where to refer inquirers.

Timing of communication needs to be carefully considered, and whenever possible, employees should be briefed in advance or simultaneously with external audiences especially when the crisis or action directly affects them. The organization's workforce can be mobilized as communication ambassadors if employees are empowered to relate approved key messages to customers, colleagues, and the community. As with other stakeholders, employees need forthright, honest, and timely information.

An organization must be sensitive, understanding, and respectful of employee needs, especially when employees question management's motives or disagree with a course of action. A disgruntled employee could go to the media and generate public attention, customer reactions, and perhaps even spur a regulatory investigation. This type of situation exploded recently at Kaiser Permanente when an employee was critical of the CEO's actions and wrote a 2,000-word e-mail tirade accusing the HMO of mismanagement. The note was sent to 120,000 staff members, creating a domino effect. In the ensuing days, the note appeared in cyberspace, negative news articles began appearing, additional investigative reporters became interested, an internal review ensued, a state watchdog agency conducted an investigation and released findings, and the CEO was forced to explain all of the issues publicly to everyone. Although not all such hostile employee actions can be prevented, engaging employees in dialogue and providing management feedback can potentially result in a more constructive solution.

There is no shortage of ways to communicate with employees today. In addition to traditional face-to-face conversations or meetings, employers can establish organizational intranets, videoconferencing, podcasts, or online meetings to facilitate rapid dissemination of information to employees across the country or around the globe.

CONCLUSION

Organizations can manage issues before they escalate into crises through preparation of a well-developed external and internal communication plan. Through the process of identifying potential vulnerabilities and developing appropriate communication strategies for stakeholders, every organization can be in a significantly better position to safeguard its reputation, instill confidence in its overall response, and put the crisis behind it.

See also Crisis Management; Crisis Management Plan; Crisis Management Team; Crisis Spokesperson; and Reputation Management.

CRISIS SENSING MECHANISM

W. Timothy Coombs

Preparation is the key to crisis management. Better preparation should translate into a more effective crisis management effort. However, you do not have to be in crisis management long to learn that preparation is not as easy as it might seem. A lot of different factors are involved in preparation including the crisis management plan, the crisis management team, and the need to practice your responses. Part of preparation is identifying and disarming potential crises, a practice that can be termed *crisis sensing*. Business security can play a vital role in identifying potential crises. The best crisis management is the prevention of a crisis. Again, it is easy to say we need to identify potential crises but much more difficult actually to do it. This entry explains what crisis sensing is and outlines a process for developing a crisis sensing mechanism that allows a crisis manager to scan and locate potential crises more effectively.

CRISIS SENSING: THE BASICS

In almost all cases it is better to prevent a crisis than to let one happen. Preventing crises saves financial resources, damage to an organization's reputation, environmental damage, and most importantly can avert injuries or deaths. In rare cases an organization may need to experience a crisis in order to make needed changes. Still a crisis is a poor means of initiating change management. To prevent a crisis, crisis managers must first identify potential crises. Steven Fink, a noted crisis expert, refers to the warning signs of a crisis as prodromes,[1] a medical term meaning early symptoms of an imminent disease or problem. This entry uses the term *prodromes* to refer to crisis warning signs.

Prodromes do not simply announce themselves to people in an organization. There must be an active search for prodromes. The organization should construct a prodrome radar and tracking system, which can be called a crisis sensing mechanism—a systematic approach to collecting and analyzing prodromal information. Information that could contain prodromes is identified, collected, and examined to see whether any prodromes do exist. The crisis sensing mechanism identifies the prodromes that require further action and continued monitoring.

The areas of issues management, risk assessment, and reputation management all rely heavily upon scanning. Hence, these three areas should be taken into consideration when developing a crisis scanning mechanism.

Issues management is a systematic approach intended to shape how an issue, a type of problem whose resolution can impact the organization, develops and is resolved. There are two types of issues of interest to organizations: political and social. Political issues involve potential legislation or regulatory decisions. These are the issues that people in government are discussing, or what is known as the political agenda. Social issues are concerns that various elements of the public are expressing. Examples include the need to improve the environment or for the organization to be socially responsible. Social issues are the matters of concern to the general public, or what is known as the public agenda. Issues management is a proactive attempt to have an issue decided in a manner favorable to an organization.

Issues management is premised on identifying and acting on issues. People cannot act on issues if they do not scan for them. The focus of issues management is thus on external issues—policy and social concerns. Many issues can develop into crises. A regulatory or legislative decision, for example, can constrain an industry through government sanctions. Seat belts and air bags are in cars because of political issues. And social issues may demand an organization alter how it operates. Consider how pressure over corporate social responsibility has changed how organizations function and report to stakeholders without any legislation or regulation involved. Moreover, social issues can become political issues. Again, seat belt and air bag regulations and laws reflect social concerns for safety.

Risk assessment seeks to identify risk factors or weaknesses and to assess the probability that a weakness will be exploited or develop into a crisis. Refer to the entry Risk Management for additional information on the subject. Common risk factors include products, regulations, facilities, personnel, the production process, competition, and customers. Risk factors exist as a normal part of an organization's operation. Risk assessment has more of an internal focus. The weaknesses identified through risk assessment offer vital information for crisis managers. For instance, safety records could show a number of minor spills while unloading dangerous chemicals. The crisis team could look at this risk as having the potential to trigger a crisis with a serious loading error. Security is a contributor to the risk assessment. Efforts to access the computer system or physically enter a facility can also be warning signs of larger events to come. (Refer to the entries Information Security and Suspicious Cyber Activities.)

A favorable reputation is a business asset at any time and especially during a crisis. Reputations are built on the relationship between an organization and its stakeholders. (Refer to the entry Reputation Management for more information on the topic and its relationship to crisis management.) If stakeholders feel neglected or are treated poorly, reputation can suffer. This includes organizational miscues such as crises. Organizations must manage a number of often contradictory demands when dealing with stakeholders. Stakeholder relationships must be monitored for problems that could impact the reputation. Reputation problems with stakeholders can escalate into crises. Customers can boycott or engage in negative word of mouth, employees can strike, activist groups can generate intense negative publicity, and the news media can create adverse publicity of its own through unflattering investigative reports. Identifying early problems in the organization-stakeholder relationship could help to avert a reputation-based crisis.

Crisis scanning benefits from the input of risk assessment, issues management, and reputation management. These three areas can be the foundation but not the only parts of a comprehensive crisis sensing mechanism. The problem facing crisis managers is how to integrate these three areas into a smoothly flowing crisis sensing mechanism.

CRISIS SENSING MECHANISM BUILDING BLOCKS

A crisis sensing mechanism has three basic elements: (1) sources of prodromal information, (2) tools for collecting prodromal information, and (3) criteria for evaluating prodromal information. This section defines and provides examples for each of these elements.

Sources of Prodromal Information

Collecting information is a vague and potentially fruitless exercise. Unless people know what sources to use, information collection is doomed. A student cannot research a paper unless he or she knows what sources exist and where to find

Crisis Scanning: Sources to Look At

The common sources scanned for crisis risks can be divided into three groups: (1) exposure concerns, (2) internal reports and audits, and (3) communication from stakeholders. Exposure concerns identify known risks that can negatively affect an organization. Organizations already collect data about each significant category of exposure. Internal reports and audits are collected data that can be relevant to crisis threats. Finally, communication from stakeholders can signal a problem that warrants attention because it could develop into a crisis.

Exposure Concerns

- Liability exposure
- Criminal exposure
- Natural disaster exposure

Internal Reports and Audits

- Security reports
- Legal compliance audits
- Safety and accident records
- Total quality management reports

Communication from Stakeholders

- Web sites and blogs
- News media
- Activist groups
- Government publications and announcements
- Internet use monitoring

them. Hence, one of the first things a new student is taught is how to use the library and other informational tools such as the Internet. Crisis managers will not find prodromes unless they know where to look for them. The Crisis Scanning box lists the potential crisis sources that an organization should monitor.

Tools for Collecting Prodromal Information

Once the potential sources of information are located, the crisis manager must know how to gather the information. Going back to our example, a student needs to know how to use the library, not just where it is physically. An essential list of collection tools would include content analysis, interviews, surveys, focus groups, and informal contacts. Detailed definitions of the collection tools are beyond the scope of this entry. Each functional area in an organization will have various ways to collect information. For instance, information security monitors and logs attempts to access an organization's network whereas customer relations monitors and logs complaints and other problems with products or services.

Criteria for Evaluating Prodromal Information

Having information is not enough; you must process the information before it is of any value to you. Processing the information converts it into usable knowledge. Crisis managers must be able to analyze the data they gather to determine whether any prodromes exist. The reason for finding prodromes early is to locate those that can significantly affect the organization and to take steps to reduce the likelihood of a crisis developing. Evaluating the information is the process of understanding if and how a prodrome might impact an organization. Let us consider some common evaluative criteria for risks, crises, and stakeholders.

Risks vary in their potential to become crises. The crisis manager must be able to tell the difference between minor risks and crisis-producing risks. Two common criteria are used to evaluate risk: likelihood and impact. Likelihood is the probability that a risk can or will become an "event"—it will cause something to happen. Impact is how badly the event could affect the organization. Impact considers such factors as disruption of organizational routines and potential damage to people, processes, facilities, or reputation. Each risk can be assigned a score of between 1 to 10 for both likelihood and impact. Those risks reaching a predetermined score will be labeled as potential crises and preventative measures taken. An organization might desire to manage all risks, but time and resources limit organizations to addressing only the top priority risks. Consider how computer-based video surveillance can be programmed to recognize where movements are a threat or a normal occurrence.

Issues and reputation threats can also be evaluated using the likelihood and impact criteria. Likelihood is the probability of an issue or reputation threat gaining momentum. An issue or reputation threat with momentum is developing and is more likely to affect the organization. Indicators of momentum include intense mass media coverage, sophisticated promotion of an issue, large number of stakeholders with the same concern, and/or strong self-interest link between stakeholders and the issue. The anti-Alar campaign illustrates issue momentum. Alar is a chemical that was used to treat apples. In less than a year, the Natural Resources Defense Council (NRDC), the primary anti-Alar group, had Alar removed from use. The NRDC hired professionals to construct the publicity effort, using sophisticated promotion. Celebrity appearances helped to generate massive media coverage. Finally, Alar was identified as a threat to small children, creating a strong self-interest link to the issue. The Alar ban inflicted significant financial losses on the apple industry. There are still debates about the real threat posed by Alar. Later studies suggested that the threat from Alar had been greatly overstated. The Kryptonite case also illustrates a reputation threat. The large number of Internet postings about the vulnerability of Kryptonite bicycle locks damaged the company's reputation and forced it into a recall of the product.

Impact is the ability of the issue or reputation threat to affect operations or profits. Impact involves the use of forecasting techniques for projecting the potential effect of the issue or reputation threat on an organization. There are myriad forecasting techniques from which to choose for issues management. Reputation threats must be assessed for their appeal to other stakeholders and the amount of communication about the threat. A reputation threat that appeals to other stakeholders and is being actively communicated is likely to inflict greater damage on an organization than a threat that has little appeal and a weak communication effort. Organizations should use those forecasting techniques with which they are most comfortable. Issues and reputation threats should be rated from 1 to 10 for both likelihood and impact. The top scoring issues should be tracked further and the organization needs to consider taking actions to prevent or lessen the threat from the issue.

Steps for Constructing the Crisis Sensing Mechanism

The following general steps for creating a crisis sensing mechanism can be adapted by each organization that applies them. No single crisis sensing mechanism is right for all organizations; each has quirks that must be taken into consideration. However, some basic idea of crisis sensing mechanism construction can be offered.

Step 1: Identify Existing Crisis Sensing Activities

Audit your organization to determine what units are already sensing the environment. To avoid re-creating the wheel, use the existing sensing activities as a foundation for your crisis sensing mechanism. Be sure to review risk assessment, issues management, and stakeholder relationship activities. Ask each organizational unit what it currently does to identify problems/opportunities internally or externally. In other words, what are its scanning activities?

Step 2: Assess the Existing Crisis Sensing Activities

You may need to develop new crisis sensing activities if the existing ones do not form a complete system. If key risk sources are being overlooked, you need to expand the crisis sensing activities. For example, if no effort is made to scan relevant activist groups, add that as a source. Make sure all possible sources you can think of are being scanned.

Step 3: Assess Information Gathering Techniques

Review how the information is being gathered. Pay particular attention to any coding systems used. A common weakness in information collection is a coding system that is too general and misses important details contained in the information. Consider an example of a retail store that codes news stories and blog entries about the organization. A general coding system would simply count the total number of positive and negative comments about the store. Such coding provides a global assessment of the reputation—is the reputation favorable or unfavorable? No insight is given into why the media image is favorable or unfavorable. A specific coding system might include categories such as sales staff, customer service, selection, merchandise quality, value/pricing, store appearance, and parking. The retail store would have separate evaluations for the seven categories. Store managers would know which exact areas of the store's reputation were strong and which needed improvement.

Step 4: Develop Procedures for Funneling Information

A crisis manager or team can neither process information it does not receive nor attend to prodromes it never knew about. Procedures must be developed for routing the information to the crisis manager in a timely fashion. Various parts of the organization will be responsible for different pieces of information. Some organizational units involved in scanning include security, operations and manufacturing, marketing and sales, finance, human resources, legal, customer communications and satisfaction, environmental and safety engineering, public relations/public affairs, engineering, shipping and distribution, and quality assurance. The different units must route their information to the crisis manager, who evaluates it for prodromes. Taking a cue from integrated marketing communication, the organization must share vital, incoming information. The crisis manager/team becomes the center of a large crisis sensing mechanism. The crisis manager/team must be treated as a functioning unit that is integrated within the flow of organizational activities and information flow.

Step 5: Establish Evaluative Criteria

Each crisis manager/team must decide how to translate these general criteria into organizational-specific criteria they can use. The crisis manager/team must decide which criteria to use, create any additional criteria that may be needed, and very clearly define the evaluative criteria. Without clear definitions, the criteria cannot be applied consistently by the crisis manager/team. For instance, what is the difference between risk impact ratings of 3, 6, and 9? The criteria must be used consistently if the crisis team is to compare and rank order the prodromes. It takes time to develop precise criteria, but the rewards are well worth the work.

Step 6: Test the Crisis Sensing Mechanism

Developing a crisis sensing mechanism does not mean it works. The system must be tested. Tests are as simple as placing selected information into the various sensing activities and seeing whether that information reaches the crisis manager and how long it takes. The crisis sensing mechanism is a complex communication/information processing system that requires regular checking and refinement in order to maintain and to improve its efficiency.[2]

CONCLUSION

We must believe that preventing crises is an important part of crisis management. To prevent crises, an organization must identify the prodromes that threaten the organization. The crisis manager/team should be in a constant state of prodrome scanning. Working with other units, including business security, a crisis team can construct a comprehensive crisis sensing mechanism for detecting prodromes. Crisis sensing mechanisms formalize procedures for funneling information containing potential prodromes to the crisis manager/team. It is worth an organization's time and effort to craft a crisis sensing mechanism because it better prepares an organization for avoiding crises.

See also Countersurveillance; Crisis Management; Reputation Management; Risk Management; and Suspicious Cyber Activities.

NOTE

1. Steven Fink, *Crisis Management: Planning for the Inevitable* (New York: American Management Association, 1986), 15-18.

2. W. Timothy Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, 2nd ed. (Thousand Oaks, CA: Sage, 2007), pp. 113–124; and W. Timothy Coombs, *Code Red in the Boardroom: Crisis Management as Organizational DNA* (Westport, CT: Praeger, 2006), pp. 65–76.

CRISIS MANAGEMENT PLAN

W. Timothy Coombs

The crisis management plan (CMP) is not a step-by-step guide on how to handle a crisis. There is no way such a CMP can be drafted; do not believe people who say they can create such a plan for your organization. At best, a CMP is a carefully arranged selection of information that can aid a crisis team. President Eisenhower once said, " . . . plans are useless but planning is indispensable." This quote captures the value of the CMP, which does not tell you how to manage a crisis but rather highlights what should be done when managing a crisis.

Time is a valuable commodity in a crisis, and the CMP is a time-saver. The CMP pre-collects some critical information for easy access and premakes some decisions by determining many responsibilities and tasks before a crisis hits. The pre-collected information includes contact information for people who may be needed during a crisis, so that time is not lost trying to figure out whom to contact and how to reach them. You also know that certain tasks need to be performed during a crisis. Team members can be preassigned responsibilities for dealing with fundamental tasks such as talking to the news media or contacting specific people. The Stakeholder Network box gives an example of identifying the people the crisis team may need to contact and how to reach them. When responsibilities and tasks are preassigned for fundamental crisis tasks, time is not lost making these basic decisions.

Speed can cause people to make errors. The CMP provides reminders of what typically needs to be done during a crisis. Of course, the exact actions are modified to fit the specific crisis facing the organization. One important concern is documenting the actions of the crisis team. This documentation is useful when evaluating the performance of the crisis team and can serve as evidence if a lawsuit follows the crisis. The CMP contains forms to remind the crisis team to document actions and provides guidance for collecting the information needed for the documentation.

CMP: A BASIC OUTLINE

CMPs can have various configurations. This section outlines a generic CMP that can be adapted for your organization. The Generic Components of a Crisis Management Plan box lists the basic elements. The Guidance Appendix also contains a sample generic CMP.

A CMP begins with a series of "official" pages: cover page, introduction, acknowledgments, and rehearsal dates. These serve to make people aware of the value of the CMP. The cover page identifies the document as the CMP, notes whether the document is confidential, and lists the date of the last revision. The introduction contains a message from the CEO that reinforces the importance of crisis management and the CMP. The acknowledgments page is completed by individuals on the crisis team and then returned to human resources. The form states the person has read and understands the CMP. The introduction and acknowledgments reinforce the importance and the seriousness of crisis management. Rehearsal dates list each time training occurred and the type of training involved.

The next section of the CMP contains the contact information. The crisis management team (CMT) list details the team members, their basic responsibilities, when the CMP should be activated (i.e., what is a crisis), and how to activate it. The CMT contact sheet has all possible contact information for the crisis team members and their alternates. (It is important to have alternates if a crisis team member is unavailable.) The secondary contact sheet lists people that might be needed during a crisis, such as the insurance company adjuster or a federal regulator.

The final section is composed of documentation materials and reminders. The crisis risk assessment is discussed in the Crisis Sensing Mechanism entry. It involves identifying and rating the various crisis risks faced by an organization. Place a table summary of your crisis risk assessment in the CMP for documentation purposes. The incident report is a record of what was done during the crisis. Key points include when the crisis was first discovered, where it happened, and when various people were contacted. The CMT strategy worksheet records all the statements personnel from the organization make about the crisis to external stakeholders. The messages are listed along with the target stakeholder(s) for

Stakeholder Network

Stakeholders are any group that can affect or be affected by an organization. In other words, stakeholders are any group that has a relationship with an organization. Stakeholders can be divided into primary and secondary stakeholders. Primary stakeholders are those whose actions can either harm or benefit an organization. The organization would no longer exist if the stakeholder withdrew its support and could not be replaced. The primary stakeholder can disrupt or completely close down an organization's operations. Typical primary stakeholders include

- Employees
- Investors
- Customers
- Suppliers
- Government agencies (national, state, and local levels)

Secondary stakeholders include any group that can affect or be affected by the organization. They can be a distraction, but they alone cannot close down an organization. The danger is if they recruit a primary stakeholder to be their ally. Typical secondary stakeholders include

- News media
- Activist groups
- Competitors

(continued)

You should know the answer to each of the following questions—not just names but how contact them:

1. Who are the reporters who might cover your organization at the local newspapers? How about at the local radio or TV stations?
2. Whom should you talk to at the local hospital to find information about injured employees who were taken there?
3. Who is the leader of the nearest environmental activist group?
4. Who is the person(s) who will lead the crisis management effort in your organization?
5. Which local emergency agencies could help in a crisis?
6. Which local government official(s) should be informed about a crisis?

It's a good idea to make a stakeholder network list—people or stakeholders you might want or need to contact about a crisis. The contact information for the stakeholder network should include

- Type of stakeholder
- Name and title of the contact person(s) for that stakeholder
- How to reach the contact person (cell phone, fax, and e-mail)
- Who from the organization has a prior relationship with this stakeholder
- Who from the organization should make contact with the stakeholder
- Documentation for the contact—note who was contacted, when, and by whom

Such a list makes it easier to reach important stakeholders during a crisis.

each message and the objective of the message. The worksheet also contains a list of technical terms that might need to be translated for stakeholders. This prevents a jargon-laden message from confusing stakeholders.

The stakeholder contact worksheet records when a stakeholder makes a request for information, who the stakeholder is, how the organization responded, and when the organization delivered the response. Often in a crisis, the team does not have the answer to a question and promises to supply it later. The stakeholder contact worksheet allows the team to track requests and ensure delivery of the promised follow-up. The business continuity plan (BCP) reference is a reminder that the company may take action to ensure that business as usual is

Generic Components of a Crisis Management Plan

1 Cover page
2 Introduction
3 Acknowledgments
4 Rehearsal dates
5 Crisis management team list
6 CMT contact sheet
7 Secondary contact sheet
8 Crisis risk assessment
9 CMT strategy worksheet
10 Stakeholder contact worksheet
11 Business continuity plan reference
12 Crisis control center
13 Postcrisis evaluation tools

maintained. The BCP is a separate document; however, it may call for changes that the crisis team will need to account for in its actions. Refer to the Business Continuity entry for additional information.

The crisis control or command center is the physical location where the crisis team will meet. This may be a dedicated room or just a conference room. Alternative sites need to be included in case the primary crisis control center is destroyed or inaccessible. The postcrisis evaluation tools are a series of interview questions and surveys that can be adapted for the postmortem of the crisis management effort. Crises are valuable learning experiences, but no learning occurs without reflection. The postcrisis evaluation tools provide guidance for learning from the crisis.

The cover page includes the date of the last revision. A CMP should be updated significantly at least annually. Major changes are needed to incorporate alterations that were recommended by previous exercise evaluations. Because organizations and personnel change, the company's risks may have changed, contact people have changed, and/or contact information has changed. Crisis managers should continually update contact information and names for the CMP, which can be sent and added to an existing CMP. There is no need to reprint the entire CMP for contact information updates.

A CMP is nearly worthless if it is never tested or updated. Management must recognize whether the CMP has serious flaws or is an effective guide for the crisis management team. The only way to know this is to test the CMP in a simulation or exercise. Organizations make a serious error when they think a CMP on a shelf in a binder is a magic insurance policy that will protect them from the ravages of a crisis.[1]

CONCLUSION

A CMP is a living document. The crisis manager must ensure it is constantly up to date. Personnel change, policies change, and buildings change. Any of these modifications can make a CMP out of date. The crisis manager is the logical person to review the CMP and make sure it has the latest information. Organizations should also think beyond the binder. Team members need to print copies of the CMP. Try different formats such as laminated, easy-to-read booklets. Also keep backups of the CMP on the organization's intranet for additional access. A CMP should be kept short, but a crisis team might need certain detailed information during a crisis, such as safety data. In that case, a crisis team can create a crisis appendix. The crisis appendix is an electronic storehouse of information that could be useful in a crisis. The Crisis Appendix box provides a further discussion of the topic.

Crisis Appendix

Crisis management plans are meant to be lean. However, there is a lot of information that would be useful to have collected before a crisis hits, such as safety data, documentation regarding regulations, and benchmarks for particular practices in your industry. The exact types of information depend upon your organization and the various crisis threats it faces. The crisis appendix to a CMP is a knowledge database for the crisis management team. This supplement to the CMP contains past crisis knowledge (what was learned in exercises and previous crises), pre-collected information, and templates (prewritten crisis messages that require only a few blank spaces to be completed).

Pre-collected information should be organized by the questions that would need to be answered in each crisis. List the questions a crisis team knows it will face, and try to collect information in advance to help answer those questions. Revise the information regularly to keep it current. Documents can range from maintenance records for machinery to policies for handling terminated employees.

Templates are predrafted statements about a crisis, such as news releases. Selected blank spaces are left to customize the messages, such as location of an incident and number of people affected. With a predrafted message, the legal team can review the documents for any legal liabilities and preapprove the messages. Any actions that can be accomplished before the crisis speeds the reaction time to the crisis—crisis teams spend less time thinking and more time doing.

See also Crisis Communication: External and Internal; Crisis Management; Crisis Management Team; and Business Continuity.

NOTES

1. American Management Association, "AMA Survey: Crisis Management and Security Issues," 2005, online at http://www.amanet.org/research/index.htm (accessed Sept. 21, 2006).

2. W. Timothy Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, 2nd ed. (Thousand Oaks, CA: Sage, 2007), pp. 66–77.

CRISIS MANAGEMENT TEAM

W. Timothy Coombs

The crisis management team handles the crisis response and develops crisis preparation plans. The team is cross functional, meaning it is comprised of people from different areas of the organization. The team meets in a designated area during a crisis and leads the crisis management effort. Ideally, the organization's full-time crisis manager guides the crisis management team. The most recent statistics reveal that only 56 percent of large companies actually have a dedicated crisis management team.[1] The three main tasks of the crisis management team are to create the crisis management plan (CMP), to enact the CMP in exercises and real crises, and to address any problems not covered in the CMP.

A CMP is only as good as the crisis management team using it. Great teams can overcome bad plans, but bad teams doom even the best CMP. A CMP is only a guide, so the crisis management team must be able to cope with whatever the crisis throws at it. A CMP helps a team cope, but the team must be ready and able to perform if the crisis management effort is to be a success. The crisis management team, not the CMP, makes the decisions during a crisis. Developing an effective crisis management team requires careful selection and training of team members. Team members must be well suited to crisis management and improve their skills through practice.

DEMANDS OF THE CRISIS MANAGEMENT TEAM

Most crisis management teams are selected based on functional areas of an organization. Each crisis management team needs certain skills and knowledge that are found in an organization's various functional areas. Common functional areas placed on a crisis management team include legal, public relations, security, operations or technical, finance, marketing, government relations, safety, quality assurance, human resources, and information technology. These areas each possess various skills and knowledge a crisis team might need, such as the ability to handle the news media or the need to assess legal consequences of an action. The exact composition of a crisis management team can vary by the nature of the crisis. Information technology is essential during a computer hacking crisis, whereas human resources is not. Those priorities shift when the crisis involves workplace violence. The core of the crisis management team includes operations or manufacturing, public relations, security, and legal. These members have skills and knowledge needed in virtually every crisis.

As in any job, certain knowledge, skills, and traits are unique to a crisis management team; these are called general crisis management skills. Two key skills are decision making and listening. Crisis management teams make decisions; that is their core function. Not all people have the knowledge and skills to make quality decisions. Bad decisions occur when a team fails to analyze the problem and improperly evaluates its alternatives to solve it. Quality decisions are typically found when a team analyzes the problem, has standards for evaluating alternatives for solving the problem, and honestly evaluates the positive and negative qualities of each alternative. Crisis management teams use listening to collect the information necessary to make decisions. Members of the team must listen to one another as well when they are involved in the decision-making process. Listening is different from hearing. Crisis teams must focus on what is being said and evaluate the information.

Certain traits are helpful or harmful to a crisis management team. One harmful trait is communication apprehension: the fear or anxiety some people feel in a communication setting. Teams making decisions constitutes a communication situation. A team member with high communication apprehension in a team setting cannot contribute to the group. Because that person does not provide information and input from his or her functional area, the desired knowledge and skill from that functional area are lost. A second trait, which is helpful, is remaining calm under pressure. Crisis management teams must make time-pressured decisions in ambiguous situations. The situation is ambiguous because the crisis management team may not have all the facts before a decision must be made. Ambiguity tolerance is a personality trait. Some people have higher tolerance for ambiguity than others. People with low ambiguity tolerance will feel increased stress in ambiguous situations. Crisis team members should have high ambiguity tolerance because they will experience less stress during the crisis.

IMPLICATIONS FOR CRISIS TEAM SELECTION

Crisis management teams should not be selected simply by functional area. Many people are excellent at their jobs but ill suited for a crisis management team, because they lack the personality traits to be effective crisis management team members. Each functional area should screen potential crisis team members for communication apprehension and ambiguity tolerance. If the knowledge and skill in the functional area is equal, pick the person with the lowest communication apprehension score and the highest ambiguity tolerance score. Refer to the Guidance Appendix for more information on screening employees for communication apprehension and ambiguity tolerance.

IMPLICATIONS FOR CRISIS TEAM TRAINING

Other entries discuss the need to train various teams in the organization, including the crisis management team. Crisis management teams should exercise or drill at least once per year. An exercise or drill offers some variation of a crisis simulation that a team must address. Most organizations do not hit this once-a-year target because of the costs and time commitment. Moreover, crisis teams should work on the general crisis team skills of decision making and listening. These training sessions can be short and, although relatively inexpensive, provide another way to help keep a crisis management team sharp and ready for action.

SPECIAL CONSIDERATION: VIRTUAL TEAMS

Advances in communication technologies have made it possible to have virtual crisis management teams. Virtual teams are when not all team members are in the same physical space with face-to-face contact. Teams can use mediated communication such as the Internet and cell phones to hold their discussions, share information, and make decisions. Most virtual teams are partially distributed groups, meaning some team members are in the same location, while others are in remote locations such as at the site of a crisis. A partially distributed team allows the crisis management team to start managing the crisis sooner. A normal crisis management team does not do much until it assembles in its designated location, the crisis center. Team members can handle some of their individual tasks, but no team action is made until the team is together. Virtual teams can begin discussions and decision making as soon as teams are en route to the crisis center. This has the potential to speed up the crisis management effort. A word of warning: A virtual team is dependent on functioning communication technology. Technical failures prevent accruing any benefits from a virtual team. Still, an organization should investigate the possibility of equipping and training crisis teams so they can sometimes take advantage being virtual teams.[2]

CONCLUSION

Crisis teams are an important resource during crisis events. The crisis team is trained in using the CMP and takes responsibility for handling the event.

Organizations should take care in how they select and train people for crisis teams. Selection should be based on a combination of functional areas and personal traits. Exercises are used to determine whether team members are ready, need additional training, or should be replaced on the team. The best CMP will fail if the crisis team is ineffectual. Too often organizations stop with a CMP and neglect to develop and train their crisis teams.

See also Crisis Communication: External and Internal; Crisis Management; Crisis Spokesperson; Exercise and Training Basics; Physical Security; Reputation Management; and Terrorism.

NOTE

[1] American Management Association, "AMA Survey: Crisis Management and Security Issues," 2005, online at http://www.amanet.org/research/index.htm (accessed Sept. 21, 2006).

[2] W. Timothy Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, 2nd ed. (Thousand Oaks, CA: Sage, 2007), pp. 66–77.

CRISIS SPOKESPERSON

W. Timothy Coombs

Some crises require one or more people from an organization to speak with the media. The typical format would be a press conference or an interview. The spokesperson becomes the voice and often the face of the organization during the crisis. The wrong spokesperson can make the crisis worse. Management must select and train spokespersons before the crisis hits.

SPOKESPERSON ROLE

A spokesperson's primary job is to provide accurate and consistent messages. Crisis experts often phrase this as speaking with one voice. This gets misinterpreted to mean that only one person speaks for an organization during a crisis. What if the crisis lasts more than a few hours? Can one person be expected to provide the message for twenty-four to forty-eight hours? The news media want to hear from experts on the subject. No one person could be an expert on all facets of the crisis. Questions could include operational concerns, employee relations, regulatory compliance, and legal matters. An organization needs to make a number of people available with each one speaking to his or her own expertise. The key to consistency is coordination. Each spokesperson should be briefed on the same background information to avoid contradictions. This does not mean each person spouts the company line. Rather, all of the spokespersons have the same information on which to base their comments.

Being a spokesperson may sound easy—just get out there and answer questions—but it is not easy to be an effective one. In addition to the pressure from the crisis is the strain of standing in front of the media and answering questions. As having helped evaluate potential spokespersons for organizations, I can tell you that not everyone can do it. Training helps, of course. Practicing answering questions in a media interview or news conference format is an excellent way to (1) determine whether a person has the potential to do it and (2) improve the spokesperson's performance.

A spokesperson has four main tasks: (1) appear pleasant on camera, (2) answer questions effectively, (3) present crisis information clearly, and (4) handle difficult questions. Appearing pleasant on camera does not mean looking good. Being pleasant refers to a set of delivery skills that allows a spokesperson to appear trustworthy and in control rather than deceitful and out of place. To appear trustworthy and in control, a spokesperson must maintain consistent eye contact (eye contact at least 60 percent of the time), use hand gestures to emphasize points, avoid a monotone by varying vocal qualities, have an expressive face, and avoid too many vocal fillers such as "uhs" or "ums." Part of spokesperson training should be to work on these delivery skills. It is critical to videotape spokespersons during training so they can see the strengths and weaknesses of their own delivery. The delivery skills do affect how people perceive the message. Of course, message content is still critical. A good delivery reinforces the message and makes it easier to understand. That is why an effective spokesperson is thoroughly briefed on what the crisis team has done and will do. A pleasant delivery will not overcome a lack of content.

Bad delivery, however, can doom even great content because it creates serious problems. First, the delivery can detract from the message. The audience gets distracted by the bad delivery and does not properly evaluate the information. Research consistently shows that bad delivery reduces message clarity. Keep the focus on what is being said, not how it is being said. Second, bad delivery can create the impression of deception. The Signs People Believe Indicate Deception box lists the factors people use to detect deception. These may not be accurate predictors, but people believe these cues are effective. In fact, the four factors on the deception list are signs of being nervous. An untrained spokesperson will look nervous and, therefore, be viewed as deceptive. Preparation and training can reduce nervousness and focus on the delivery factors that create a positive impression.

HOW TO HANDLE QUESTIONS

An effective answer to a question is one that answers the question that is asked. Some consultants emphasize getting your message out by answering the question you want rather than the one that was asked. This is dangerous, because the

Signs People Believe Indicate Deception

1. Avoiding eye contact
2. Frequent use of vocal fillers such as “ums” and “uhs”
3. Nervous gestures or repetition of a gesture, such as touching one’s face
4. Too many hand gestures

spokesperson appears evasive. Always answer the question you were asked first. If the question provides an opening to state a set message the organization would like to make, add it to the end of the answer. A spokesperson can also provide this set message during the introductory remarks given before taking questions. Listen to the question and answer that question.

The odds are that reporters will ask a question that the spokesperson does not have an answer for, which is fine. Say that you do not know and will get them the answer as soon as you can. Do not use the words “no comment.” People hearing “no comment” assume the company is guilty and trying to hide something. Reporters can get hostile and try to bait the spokesperson. One form of baiting includes asking the spokesperson to speculate on things such as the cause of the crisis. Do not speculate in a crisis. If you speculate and are wrong, the organization looks deceptive or incompetent, neither of which is good for the organization. Keep your composure and do not argue, even if the reporters are hostile. You will lose the argument and look bad. Never forget: Reporters have the last word, because they write the stories.

A spokesperson’s answers must be clear and easy for the reporters to understand. This means avoiding jargon and technical terms. Every job has its jargon and technical terms. People in those jobs understand this language but those outside do not. In addition to being unclear, too much jargon and technical language can be interpreted as sidestepping a question. The reporters may believe the lack of clarity is intentional and being used to hide something.

MANAGING TOUGH QUESTIONS

If you have ever seen a press conference, you know that not all questions are equal. The difficult ones include questions that (1) ask more than one question, (2) are long and complicated, (3) are based on erroneous information, (4) are multiple choice with unacceptable options, and (5) are tricky and tough. A spokesperson needs to recognize the tough question and respond strategically. Any practice sessions should include some tricky questions.

When asked a question that is really multiple questions, a spokesperson has two options. The first option is to select one of the questions and answer that one.

Reporters can ask follow-up questions if they really want an answer to another part of the question. The second option is to address all parts of the question. The spokesperson may want to write down a few quick notes to keep track of the multiple parts of the question. For a long and complicated question, the spokesperson can ask for the question to be repeated, which gives the reporter a chance to clarify the question. Another option is to paraphrase the question and ask the reporter whether that is an accurate read on the question. Each option creates clarity and provides the spokesperson some additional time to formulate a response.

If a question is based on erroneous information, challenge and correct the information. Misinformation must be corrected immediately, or it will become a "fact" in the story. When a question has multiple-choice options that are all bad, the spokesperson should explain how the options are inappropriate and offer his or her own option as the answer. Finally, if a question is tough or tricky, the spokesperson must find a tactful way of saying so. It may be that the question cannot be answered. Explain why you cannot answer it and go to the next question. Do not turn either of these last three tough questions into a confrontation. Offer a correction or response in a pleasant tone and move on.[1]

SPOKESPERSON PREPARATION

Both training and briefing sessions are used to prepare spokespersons. Training sessions involve practicing answering questions. Those sessions are taped and then critiqued by the spokesperson and others on the crisis management team. The organization's crisis manager should develop the training crisis scenarios and questions. Briefing sessions occur before actually meeting with reporters. The spokesperson is given a summary of what is currently known about the crisis, including the actions taken by the organization, a set of questions the reporters might ask, and key messages the crisis team would like to be delivered. If there is time, the spokespersons can rehearse their opening remarks and answer some sample questions.

CONCLUSION

Some crises will demand the use of crisis spokespersons. Crisis spokespersons speak for the organization during a crisis. They are selected based upon their expertise and their ability to answer questions from the news media effectively. Not everyone makes an effective crisis spokesperson. The organization must carefully select, train, and prepare each crisis spokesperson to maximize the benefits these individuals can provide during a crisis.

See also Crisis Communication: External and Internal; Crisis Management; and Crisis Management Team.

NOTE

1. W. Timothy Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, 2nd ed. (Thousand Oaks, CA: Sage, 2007), pp. 78–87.

UNCOMMON BUSINESS SECURITY CONCERNS

The topics in this final section would not jump to the front of someone's mind when asked to think about security concerns. However, these issues do have important connections to security. The emphasis on ethics reflects its growing significance across all organizational activities.

CORRUPTION AS A BUSINESS SECURITY CONCERN

W. Timothy Coombs

December 9 is world anticorruption day. Most companies do not spend much time on or give much thought to corruption. That is an issue for governments, right? Wrong. Corruption is a business issue and a business security concern. Corruption has significant financial ramifications. The U.S. Department of Commerce estimates that from 1994 to 2002, 474 international contracts were influenced by bribes. The contracts represented a total of $237 billion.[1] This entry explains what corruption is, how it affects businesses, and efforts that companies can take to reduce corruption risk.

The pressures surrounding corruption continue to grow. As more companies become international, corrupt officials still exist and can help a company seeking to expand international trade or investment. More companies are being tempted, and the pressure to give in to temptation is intensifying. But so are the forces of transparency that can unmask corruption. The Internet and satellite television make once hidden actions very visible. Companies pay a high price for corruption revelations because the exposure damages their reputations. Refer to the Reputation Management entry for a discussion of the value of a company's reputation. There is an increased risk of exposing corruption as well.

CORRUPTION: DEFINITION AND CONNECTION TO BRIBERY

The most common definition of corruption is the abuse of public position for private gain. This evokes images of politicians taking bribes. The focus in on what is called public/private corruption. Businesses, as part of the private side, are drawn into the equation when they are asked to provide the bribe money. Corruption can also be the abuse of commercial position for personal gain. This is called private/private corruption. An example would be suppliers using part of their fees as a kickback offered to the people who helped them to land the contract. Corruption involving business focuses on bribes.

Not all corruption is on the same scale. Grand corruption involves large bribes that can reach into the millions of dollars that are used to secure commercial contracts or some other business advantage. Petty corruption involves small amounts of money, typically under $100, which are often called facilitation or facilitating payments. These payments assist routine transactions such as installing utilities or passing customs inspection. Petty corruption is frequently in a gray area that is not covered by many anticorruption and antibribery conventions. Corruption is not limited to the exchange of money, because bribes can include goods, services, and jobs.

Bribes can be direct and indirect. The preceding discussion of corruption covered direct bribes given directly to the person who helps the business. Indirect bribes create yet another gray area for businesses. With an indirect bribe, the organization pays some agent or intermediary who helps negotiate a deal. This agent is paid a fee based on a percentage of the contract. Part of the commission is then given to a government official. So the bribe is indirect through the agent. Anticorruption efforts target both direct and indirect bribery.

Corruption includes an element of unacceptable influence. Personal connections, for instance, play a role in business around the world. We can find terms for business connections in China, Japan, and Pakistan, to name but a few countries. So when does a connection become unacceptable? Influence crosses the line when it becomes favoritism and lacks transparency. Favoritism indicates decisions are not fair and not in the public interest, whereas a lack of transparency means the decisions are hidden from public view. Managers need to ask themselves, "Would this action embarrass the company if it were made public?" Are you worried that the decision might appear unfair or dishonest? If the answer is yes, odds are the influence is unacceptable. Avoid actions that would harm a company's reputation. Corrupt actions injure the company's name by damaging its integrity and creating the appearance of unethical practices. The Saybolt International Case Study illustrates many of the problems corruption creates.

Corruption Case Study: Saybolt and Panama

Saybolt International is a Dutch company that tests petroleum. Its subsidiary in Delaware is Saybolt North America. The company analyzes bulk materials including oil and marks octane levels for freighters as they move from port to port, from seller to buyer. One of the areas Saybolt inspects is the Panama region. In 1995, a problem arose as the company needed to find new space for its offices and lab facilities. Saybolt lacked a long-term lease and found its facility could be taken over by the Panamanian government at any time. This problem fell to David Mead, the CEO of Saybolt North America. Then came the solution: an offer for a permanent lease for a facility in the free trade zone.

The initial message was an e-mail from an American employee working for Saybolt North America in Panama stating the new location was needed and better than the old location. However, a government official was asking for $50,000 to make the lease happen. The employee told Mead that was normal in this region. In October, Mead began talking seriously about the "fee" payment with the employee in Panama and others at Saybolt. Mead was told by one trusted source that the bribe would not violate the U.S. Foreign Corrupt Practices Act if the money were sent from the head office in the Netherlands. The actions of Mead and others involved were documented through e-mails and other correspondence inside Saybolt. Around December 21, 1995, the money was sent to the employee in Panama and a check written to the government official.

The United States government and courts had a different interpretation of the incident. They did view it as a violation of the U.S. Foreign Corrupt Practices Act. U.S. officials discovered information about the bribe a year later while investigating environmental violations by Saybolt. Mead was arrested in January 1998 and lost his position at Saybolt. Convicted by a grand jury

(continued)

for violating the U.S. Foreign Corrupt Practices Act, Mead was sentenced to four months in prison and four months' house detention. He served the time and paid a $20,000 fine.

Saybolt was fined a total of $4.9 million for the violation. A lead Justice Department prosecutor had this to say about the case: "Foreign bribes simply cannot be treated as a cost of doing business. This case demonstrates that the U.S. government will vigorously prosecute U.S. executives who give a green light to the bribing of foreign officials. Corporate executives will go to jail if they authorize these types of bribes."[2] Saybolt paid a high financial and reputation price for a $50,000 bribe that did not even pay dividends. The government official never did provide Saybolt with the agreed-upon lease.

WHAT MAKES COMPANIES VULNERABLE TO CORRUPTION?

In many countries, people assume bribes are part of the cost of doing business. The belief is that everyone does it. As parents tell their children, just because everyone else does it does not mean you should do it too. But why do companies give in to this temptation? Management style is a critical factor. Management must value and promote integrity to prevent the temptation of bribery. This includes management speaking about the importance of integrity, supplying training for employees who will be exposed to ethical dilemmas, and providing communication channels for employees that may have questions about ethics. (We will return to these concerns with the discussion of ways to prevent corruption.)

Some industries have a greater potential for bribery than others. Industries that have very expensive contracts and can benefit from the help of individual officials are at greater risk. A survey by Control Risks found that the construction, telecommunications, oil, gas, and mining industries are most likely to encounter corruption.[3] A final vulnerability factor is the political structure of a country. Countries that lack checks and balances, such as a powerful judiciary or a free and inquiring news media, are more apt to expose companies to corruption. Officials are more likely to ask for bribes if there is not a mechanism to hold them accountable for their actions. As corruption expert Robert Klitgaard puts it: Corruption = Monopoly + Discretion – Accountability.[4] If the legal system cannot help a company facing corrupt practices, it is easier to go along with these practices than to fight them. Courts and a free press can hold officials accountable and reduce the threat of corruption.

WHY IS CORRUPTION A RISK/BUSINESS SECURITY CONCERN?

As noted earlier, being caught in a corruption scandal hurts a company's reputation. But there are business risks even if the corruption can go undetected. Again, just because corruption is commonplace in a society does not mean there are not negative business consequences for following the crowd.

Corruption has financial costs for a company. Managers estimate corruption adds at least 10 percent on to operating costs. Engaging in corruption places a company at risk for future costs. The person taking the bribe gains a power over the company paying the bribe. The bribe taker can demand additional money or favors from the company, which is not in a strong position to resist those demands. Both grand and facilitation bribes (small amounts that speed up legitimate transactions) can result in repeat demands for more. Resisting additional demands can result in violence against the company. The bribe taker may become angry over lost revenue and react with violence, a clear risk to business security. Even a company's own employees can get in on the act. Workers who learn of the bribe can use the information to blackmail management. Management must either pay the blackmail or reveal its misbehavior to stakeholders.

Bribes cannot guarantee results. The company has no control over the outcome. If the bribe taker does not deliver, there is no one to complain to about it. One manager learned this lesson the hard way when trying to apply for a license for distributing a product. A government official offered him two envelopes, one marked "yes" and the other "no." The manager took the envelope marked "yes," which contained information about a Swiss bank account and a recommended fee. The fee was paid but the license never appeared.

Another set of risks involves political changes in a country. When the person taking the bribes leaves office, the connection and favors are gone. If that person is forced from office, the risk intensifies. The company becomes associated with the old, corrupt regime and will find dealing with the new government much more difficult. If the government changes because of a revolution, the bribe-paying company will be viewed as the enemy. A variety of political risks is tied to bribery.

Finally, there is a social cost to corruption, as it harms people living in the corrupt countries and other places. Corruption is clearly linked to economic harm because it hurts economic development and foreign direct investment. Corrupt governments siphon off money that could have been used to improve a country and bolster its economy. Investors hesitate to invest in companies rife with corruption because of the poor returns. Corruption can harm innocent people as companies provide substandard work to recoup corruption payments. The environment can suffer as well. Sometimes bribes are used to circumvent environmental laws. The EITI: Benefits of Reducing Corruption box extends the discussion of the social impact of corruption.

EITI: Benefits of Reducing Corruption

EITI is the Extractive Industries Transparency Initiative. This coalition of governments, companies, civil society groups, investors, and international organizations works to improve governance in resource-rich countries through the full publication and verification of company payments and government revenues from oil, gas, and mining. The following description, from the EITI web site, explains the benefits of transparency:

> The primary beneficiaries of EITI are the governments and citizens of resource-rich countries. Knowing what governments receive, and what companies pay, is a critical first step to holding decision-makers accountable for the use of those revenues. Resource-rich **countries** implementing EITI can benefit from an improved investment climate by providing a clear signal to investors and the international financial institutions that the government is committed to strengthening transparency and accountability over natural resource revenues. **Companies and investors**, by supporting EITI in countries where they operate, can help mitigate investment risk: corruption creates political instability, which in turn threatens investments which are often capital intensive and long-term in nature. **Civil society** can benefit from an increased amount of information in the public domain about those revenues that governments manage on behalf of citizens, thereby increasing accountability and improving transparency. In summary, implementing EITI as part of a programme of improved governance will help to ensure that oil, gas, and mining revenues contribute to sustainable development and poverty reduction.[5]

CORRUPTION REFORM EFFORTS

Because of its social and economic harm, corruption is drawing increased attention around the world. Governments, intergovernmental agencies, and nongovernmental organizations (NGOs) have launched a variety of anticorruption efforts. The United States has instituted the Foreign Corrupt Practices Act. The World Bank and the United Nations have targeted corruption with various policies and guidelines. The Organisation for Economic Cooperation and Development has an antibribery effort, while the Council of Europe has in place twenty guiding principles about corruption. Important anticorruption efforts among NGOs include Transparency International and the International Chamber of Commerce.

It is important to note from this discussion that corruption is now a serious business topic around the globe. Various agencies and groups are monitoring and revealing corrupt practices. The World Bank maintains a blacklist of companies that have been found guilty of involvement in corrupt practices. Over sixty-one companies have been placed on the list since 1999. A company on the list cannot compete for new work from the World Bank. This listing can be permanent or for a specified period of time. The focus on anticorruption increases the reputational risk if members of an organization lapse and engage in corrupt practices.

ANTICORRUPTION POLICIES FOR COMPANIES

Anticorruption policies should be part of a company's code of conduct. Most U.S. companies have codes of conduct that outline appropriate and inappropriate actions for employees, suppliers, and subcontractors. Two ingredients are critical to anticorruption efforts: (1) organizations having formal policies and (2) management actively practicing the policies. Having a written policy is the starting point for combating corruption. However, as many entries have noted, a written policy is not enough in an organization. Management must live the policies for them to have meaning. As noted earlier, this includes talking in support of the anticorruption policies and providing training for employees. Anticorruption training is a smart investment for a company. An active training program can be a defense when an employee violates the anticorruption policies. In the United States, penalties against a company caught using bribes are reduced if the company can demonstrate employees were trained in the anticorruption policies.

Anticorruption policies should cover six points: (1) bribes, (2) intermediaries, (3) facilitation payments, (4) gifts, (5) suppliers, and (6) conflicts of interest. An anticorruption policy must forbid any bribes. Well over 80 percent of European and 92 percent of U.S. companies include statements prohibiting bribes in their codes. Bribes are the easy part, however; the other five areas create most of the corruption headaches for companies.

Intermediaries work on commission and have been known to use part of that commission for bribes. Intermediaries are often a necessity in international business, because they possess the local knowledge required to complete deals and bid for contracts. But companies can experience legal and reputation damage when intermediaries provide indirect bribes. In the United States, Triton Energy was charged with illegal payments when an intermediary bribed officials. The U.S. government believed Triton had a strong likelihood of knowing part of the money would be used for bribes. Triton paid a $300,000 fine but did not admit to or deny the charges. A company's anticorruption policies must specify that intermediaries are not to use any of the money for bribes. Companies should request documentation from the intermediary about how the funds were used. Moreover, contracts with the intermediaries should specify the agent understands the company's anticorruption policy, provide for termination of the contract without compensation if the policy is violated, and establish the right to audit the agent's expenses and invoices.

Facilitation payments, sometimes called grease, are small amounts that speed up legitimate transactions. Though small, they are still a form of bribery, and anticorruption policies should forbid them. Companies often overlook grease because it reduces delayed paperwork, and delays increased costs. Still, once a small bribe is paid, what is to stop officials from asking for larger ones? Some companies and even certain laws such as the Foreign Corrupt Practices Act recognize grease may be allowed under certain conditions. Those conditions include that the payment is customary and of low value, is approved by senior management, does not violate any laws, is reported immediately, and is recorded in company records. The idea is to be open with the transactions. Special training is required to prepare employees who will face requests for grease.

Gifts and business entertainment are commonplace but run the risk of a form of bribe when they are excessive. It is difficult to ban gifts because gift giving is part of many business cultures. The company's anticorruption policy must set limits for gifts and entertainment. An example would be establishing a financial limit; a gift is acceptable as long as it is below a given amount. Entertainment can follow the same idea of setting a financial limit. Copies of your company's gift and entertainment rules should be given to suppliers and business partners so they know the rules too.

Suppliers sometimes pay a kickback to people at the company. Kickbacks are a type of bribe. Specify no kickbacks in the anticorruption policy, and use accounting and monitoring procedures to ensure this rule is not violated. Finally, avoid conflict of interest at all times. It is inappropriate to be involved in a business decision that affects a relative or close friend. Employees should know they must remove themselves from any decisions involving people close to them. Such situations create conflicts between the employee's company and loyalty to a friend or family member.

Best practices suggest an anticorruption policy should be thorough, written, communicated to employees through documents and training, and reinforced by management personnel. Although anticorruption policies cannot eliminate all violations, they do make it easier for employees to resist the temptations of corruption by providing clear guidance and reinforcing penalties for lapses in judgment.[6]

CONCLUSION

The term *corruption* too often is associated only with governments. Corruption is a business concern that includes governments or just other businesspeople. Corruption is related to business security and can have a direct connection to physical safety. Increasingly, international organizations are seeking to reduce corruption. Organizations are well advised to create and promote their own anticorruption policies.

See also Crisis Management; Ethics as a Business Security Concern; Ethical Conduct Audit Reputation Management; and Types of Crises.

NOTES

1. John Bray, "Facing Up to Corruption 2007: A Practical Business Guide," 2007, online at http://www.crg.com/pdf/Facing_up_to_corruption_2007_englishreport.pdf (accessed 12 Feb. 2007), p. 13.

2. Maki Hishikawa, "The FCPA: An Outgrowth of Corporate Scandals," March 2003, online at http://www.dbtrade.com/publications/the_fcpa.htm (accessed 3 March 2007).

3. Bray, "Facing Up to Corruption 2007," pp. 11–12.

4. Bray, "Facing Up to Corruption 2007," p. 13.

5. Extractive Industries Transparency Initiative, "About EITI," online at http://www.eitransparency.org/section/abouteiti (accessed 12 Feb. 2007).

6. Bray, "Facing upto corruption 2007," pp. 33–42.

COMPETITIVE INTELLIGENCE

W. Timothy Coombs

It is estimated that 90 percent of the information a company needs to know about its competitors when making decisions can be collected legally and ethically from public sources. Public sources include information disclosed to government agencies, news media reports, and interviews with people who have knowledge of the organization. Legally collecting and analyzing information about competitors and markets is the realm of competitive intelligence. Competitive intelligence provides timely, relevant, accurate, and unbiased intelligence on potential threats to an organization's competitive position. Competitive intelligence is not the illegal world of stealing information from competitors. Illegally or unethically gathering information is industrial espionage. Competitive intelligence is a rapidly growing professional field. Its growth is tied to the strong and positive connection between competitive intelligence and company performance. Companies that utilize competitive intelligence outperform competitors in the areas of sales, market share, and earnings per share. Competitive intelligence helps a company gain an edge over its rivals.

COMPETITIVE INTELLIGENCE: THE PROCESS

Broadly, competitive intelligence involves monitoring the company's competitive environment, including customers, competitors, political and legal developments (regulations and laws), and social forces (changes in norms and values). The two main tasks are the collection and the analysis of intelligence. Competitive intelligence should be viewed as a cycle of five steps. The first step is planning and direction. The competitive intelligence personnel need to meet with company decision makers to determine what type of intelligence they need. Competitive intelligence must be focused if it is to be effective. The second step is the collection of the intelligence. The collection must be done through legal and ethical means. The third step is analysis. The data must be interpreted and translated into usable knowledge. Analysis typically involves generating a list of recommendations.

The fourth step is presenting the information to decision makers. The competitive intelligence unit must explain its findings to the decision makers. The fifth and final step is feedback. The competitive intelligence personnel solicit responses from the decision makers and use that information to refine future intelligence-seeking efforts.

To be more precise, what we have talked about so far is active competitive intelligence, which includes seeking information about strategy, tactics, targets, and technology. Competitive intelligence provides insights into your rivals' intentions and marketing developments. Decision makers can translate this intelligence into strategies to improve a company's competitive position. Defensive competitive intelligence—preventing competitors from collecting information about your organization—is discussed later in this entry.

COMPETITIVE INTELLIGENCE: FAILURE AND SUCCESS

Just because a company engages in competitive intelligence does not mean it will be successful. Competitive intelligence failures have been traced to four factors: (1) resources, (2) structure and process, (3) competitive intelligence understanding, and (4) attitudes. The competitive intelligence unit may lack the funds, personnel, or skills to execute its tasks properly. Another problem with resources is that other departments might send flawed data to the competitive intelligence unit. Structure and process deal with how competitive intelligence is done. Due to the lack of best practices, there are no agreed-upon standards on how to perform competitive intelligence. Others in the organization may not understand what competitive intelligence is supposed to do. As a result, the competitive intelligence unit may waste time handling tasks that are unrelated to its core function. Attitude is a critical problem. Others in the organization often do not trust the competitive intelligence unit. They view competitive intelligence as unethical and do not consider it an essential part of the organization. Both attitudes result in the competitive intelligence unit not receiving the information it needs from other departments.

Effective competitive intelligence involves taking actions to counteract the reasons for failure. Top management must support the competitive intelligence unit with proper resources and endorsements. The resources ensure that the competitive intelligence unit has the needed funding and skilled personnel to be effective. Endorsements reinforce the competitive intelligence unit's value to the organization. The competitive intelligence unit must correct misperceptions about its activities. This involves educating others in the organization about the role of competitive intelligence (what it is supposed to do) and the ethical guidance of the discipline. The competitive intelligence unit must review current practices and develop a set of guidelines for what constitutes effective competitive intelligence. This would include identifying the resources commonly used in competitive intelligence.

SOURCES OF INTELLIGENCE

Competitive intelligence personnel utilize four main sources of information: (1) networks of people, (2) the Internet, (3) publications and public records, and (4) trade shows. Research across a wide range of business functions shows that the more people you have, the easier it is for people to get the information needed to do their jobs. Those in competitive intelligence must be in touch with other employees who have contact with customers, potential customers, suppliers, business partners, or competitors. The sales force is the top priority because it is so close to customers. Competitive intelligence should also stay close to other competitive intelligence personnel in nonrival companies. These fellow competitive intelligence people could prove to have useful data.

The Internet is an amazing collection of useful information surrounded by useless garbage. Most of the information competitive intelligence practitioners seek on the Internet is free. The focus should be on competitors' web sites where you can find financial information, job announcements, news releases, product information, and more. A second area to examine is the consumer generated media or social media that discuss your industry, your competitors, or your company. This includes newsgroups, discussion groups, and weblogs (blogs). Ideally you want social media created by customers, investors, or employees. And you can find all of these groups talking online. Social media require careful vetting of sources and information. Anyone can and does post messages to the Internet. The skilled competitive intelligence person separates the nuggets from the worthless gravel. Competitors of Ford would be wise to monitor the BlueOvalNews.com web site (http://www.blueovalnews.com/), where devoted Ford owners talk about Ford products and have been known to release new product information before Ford does. Complaint portals are another useful Internet source. As the name implies, customers post complaints about products or services. Check sites such as PlanetFeedback.com to see what customers are saying about competitors and your company.

The Internet has some commercial databases that a competitive intelligence person may want to pay for to secure access. These include Hoover's, Dunn & Bradstreet, and LexisNexis. All three offer searchable databases that contain competitor information.

Publications and public records are a mix of online and hard-copy sources. Newspapers can be a source of information about hiring. Business- and industry-specific magazines can include profiles of competitors and their products. Public records on the local, state, and federal levels can yield the following information: production capacity and expansion plans; equipment types, sizes, and materials of construction; repair and maintenance strategy; site layout and potential for expansion; raw material types and quantities; capital and operating costs; staffing levels and organizational structure; trademark and patent applications; and transportation and parking permits.

Government publications and web sites can provide useful intelligence on your industry and markets as well as some competitor data. Companies are required to file a wide range of information. For instance, the Securities and Exchange Commission (SEC) requires disclosure anytime a publicly held company does something that can affect its stock price, in addition to quarterly filings.

Trade shows are a time when companies promote themselves openly rather than hiding information. A competitive intelligence staff member can register as a participant and collect intelligence by walking, talking, and listening. By visiting the trade show booths of competitors, an individual can collect brochures, product samples, product specifications, prices lists, or white papers. The person has a chance to talk with the vendor and ask questions. The staff at the booth are usually marketing and sales staff eager to talk about the company, its products, or its services. Some trade shows have a convention element whereby vendors give presentations or speeches. Attend the presentations and speeches given by your competitor. There are also social events that present another opportunity to talk to representatives of your competitor.

Some other miscellaneous sources of competitive intelligence include competitor's advertisements, observing a facility, visiting a business, and interviews with former employees or customers. Observations should be conducted from public space to avoid trespassing. Observational intelligence can include the number and types of deliveries or the number of cars in the parking lot. You can visit public access facilities such as stores and restaurants. Buy the products or use the services to get a better understanding of their strengths and weaknesses. Finally, competitive intelligence personnel can interview people with knowledge of the competitor. These can include former employees, customers, or clients.

DEFENSIVE COMPETITIVE INTELLIGENCE

Defensive competitive intelligence tries to make it more difficult for competitors to find useful information about your company. The focus is on legal and ethical means of collecting data because the point is to block competitive intelligence efforts. The cornerstone of defensive competitive intelligence is awareness. Your employees should be aware of basic techniques that can be used to collect competitive intelligence. The first part of defensive competitive intelligence is for the competitive intelligence unit to review your company for potential sources of data for your competitors. Then employees can be trained in ways to protect this data. An example would be trade shows. Employees should know that competitors might use the trade show for competitive intelligence. Employees can ask more questions to determine whether an individual is really a potential client or a competitor seeking competitive intelligence.

The legal department is a vital part of competitive intelligence. Nondisclosure agreements (NDAs) and noncompete agreements are useful resources in tandem with an aggressive trade secret program. *Security Magazine* provides an illustration of legal protection. A burger franchise discovered a competitor kept learning of its new products and undercutting its new product launches with similar products at lower prices. The problem was a franchisee. The company had a noncompete clause stating a franchisee could not also own a competitor's franchise. However, a few franchisees were exempt because they had owned multiple franchises prior to the agreement. One of those franchisees was feeding the new product information to the competition. The company had failed to mark the material confidential, giving the franchisee a legal way out. The company learned to mark all such materials as "company confidential," "not for redistribution or for public release," or "not for public release before a specified date." See the Information Classification box for more about this subject.[1]

Information Classification

Part of defensive competitive intelligence includes an information protection program. Your company must decide what information needs protection and requires classification. Classifying information limits who has access to that information and how it is to be used. There are four common information classification categories:

1. *Personnel confidential* covers parts of employee records that should be subject to general disclosure.
2. *Business confidential* covers information that has commercial value to competitors but would not be included by the Uniform Trade Secrets Act.
3. *Special control* covers information included under the Uniform Trade Secrets Act and information about projects in the early stages of development.
4. *Security sensitive* covers information that others could use to circumvent or compromise a company's security systems and measures.

Competitively Sensitive Information

Defensive competitive intelligence seeks to cloak competitively sensitive data. So how do you determine whether data are competitively sensitive? *Security Management* offers a list of six questions to help you understand the answer.

1. What information would be the most difficult for your competition to develop on its own?
2. What information would be vital for someone constructing a competitive profile of your company?
3. What information already has some protection?
4. What information is critical your operations?
5. What competitive intelligence is your company trying to collect about its rivals?
6. What are the most common data analysis techniques in your industry, and what information is needed to complete those analyses?[2]

Once the competitive intelligence unit has examined your company, it is time to move to the second part of defensive competitive intelligence, known as cloaking. Cloaking refers to efforts to screen your organization's information from the eyes of competitors. There is no way to make your company completely invisible. Many pieces of information useful to your competitors must be publicly disclosed. Cloaking is a collaboration between competitive intelligence and security. The first part of defensive competitive intelligence locates the channels competitors use to gather data about your company. Cloaking tries to control each of those channels. The focus should be on the information that would of the greatest use to your competition. The Competitively Sensitive Information box reviews criteria for picking the critical data to protect. In addition, the competitive intelligence personnel should determine how the competitors might evaluate the data. By knowing how the data might be analyzed, your company could try to release the information in such a way as to make the analysis more difficult. Cloaking, like security, is an organizational effort. If employees are lacking in their cloaking efforts, competitors will get the information they want in the format they desire.

CONCLUSION

When executed appropriately, competitive intelligence improves an organization's competitive position. The bulk of the information needed for competitive intelligence is available from public sources and is easy to collect ethically. Employees should know what the competitive intelligence unit does and does not do to prevent misperceptions. Moreover, the competitive intelligence unit can help explain to employees what they can do to make it more difficult for competitors to gather information about their own organization.

See also Corporate or Industrial Espionage; and Ethics as a Business Security Concern.

NOTES

1. John J. McGongale and Carolyn M. Vella, "I Spy Your Company Secrets," *Security Management*, Feb. 2007, pp. 64–70.

2. McGongale and Vella, "I Spy Your Company Secrets," pp. 66–67.

ETHICS AS A BUSINESS SECURITY CONCERN

W. Timothy Coombs

Ethics concerns appropriate and inappropriate behaviors. In business, ethics is an applied practice rather than a philosophical debate. Employees need guidance on how to behave. Ethics is often tied to compliance with laws and regulations because they share a focus on what should and should not be done. Ethics and compliance programs guide employee behavior. Employee misbehavior can damage a reputation, result in fines, cost the company contracts, and result in employees being sent to prison.

Ethics and compliance programs cover behaviors related to compromising the following: customer or marketplace trust, shareholder or organizational trust, employee trust, supplier trust, and public or community trust. The Range of Behaviors for Ethics and Compliance Program box lists the more specific behaviors that are covered. Ethics and compliance tie into a number of other factors including corruption, crisis management, legal exposure, and security breaches. Clearly ethics is a business risk that needs to be managed.

Range of Behaviors for Ethics and Compliance Program

Here are examples of misconduct made possible by ethically challenged employees:

- False or deceptive sales practices
- False or misleading invoices given to customers
- Anticompetitive practices such as price fixing

(continued)

- Illegally or unethically collecting competitive intelligence
- False product quality or safety test results
- Breach of customer or client privacy
- Failure to get approval before executing customer contracts
- Violation of customer contracts
- Reporting false or misleading financial information
- Stealing or misusing assets
- False time and expense records
- Breach of computer network or database controls
- Mishandling proprietary or confidential information
- Violation of document retention rules
- Giving inappropriate information about investors or analysts
- Engaging in insider trading
- Engaging in activities that are a conflict of interest
- Wasting or mismanaging company resources
- Discriminating against employees
- Sexually harassing employees
- Violation of workplace safety or health rules
- Violation of employee benefits, wages, or overtime rules
- Violation of employee privacy
- Substance abuse at work
- Violation of supplier selection rules
- Accepting inappropriate gifts or kickbacks from suppliers
- Failure to keep accurate records of supplier payments
- Failure to get approval before entering into supplier agreements
- Violation of intellectual property rights of supplier or its confidential information
- Violation of a supplier contract
- Violation of environmental regulations
- Exposing the public to a safety risk
- Giving false information to regulators
- Making inappropriate financial contributions
- Paying bribes to government officials
- Use of a third party to provide bribes to government officials
- Violation of international trade restrictions or embargoes
- Violation of international labor laws or human rights

WHY WORRY ABOUT ETHICAL MISCONDUCT?

In 2006, the consulting firm of KPMG released a study examining misconduct in the workplace. The results served to reinforce the need for ethics and compliance programs. Of the employees asked whether they had personally seen or had firsthand knowledge of misconduct in their organizations over the past year, 74 percent answered affirmatively. The leading industries for misconduct were global manufacturing (80 percent), energy and chemicals (78 percent), and electronics, software, and services (76 percent). Employees reported a variety of misconduct including false and deceptive sales practices, mishandling confidential or propriety information, wasting or abusing organizational resources, violating workplace safety rules, discrimination, breaching computer controls, and violating environmental standards.[1] These behaviors are serious matters, not mischief, and management should work to reduce them.

There are legal reasons to be concerned about ethics as well. Section 404 of the Sarbanes-Oxley Act of 2002 covers in part an issue of ethics and compliance as well as financial reporting. Ethics and compliance programs can serve as a mechanism for reducing organizational penalties when an employee misbehaves. In the United States, federal sentencing guidelines allow for penalties to be reduced if the company has an effective ethics and compliance program. An effective program has been implemented rather than being only on paper, has mechanisms to enforce the program, has staff that evaluates compliance, and is actively communicated to employees.

The KPMG study also found that having a compliance program reduced misconduct and encouraged prevention. Employees with ethics and compliance programs reported seeing less misconduct, felt less pressure to engage in misconduct, believed in reporting misconduct, and thought management would take appropriate actions when told about misconduct.

ETHICS AND COMPLIANCE PROGRAMS

Each company faces unique risk factors, so no one ethics and compliance program is perfect for every organization. However, we can identify the basic elements used in an ethics and compliance program. Before discussing program elements, it is instructive to consider the causes of misconduct because the solutions should address the root causes.

The root causes of misconduct can be traced to job pressures and ineffective policies. Employees report pressure to do whatever it takes to meet business goals, including cutting corners and misconduct. The pressure is compounded when employees lack the resources to conduct their work properly. Employees begin to fear for their jobs if they do not engage in misconduct and believe management will reward them for their results and not worry about how they achieved those results. The ethics and compliance polices can be source of misconduct as well. Many employees do not understand how the standards apply to their jobs. Employees consider it easy to get around the rules and believe their companies do not take the ethics and compliance policies seriously. An effective ethics and compliance policy must be able to counteract both of these two negative forces.

The U.S. Department of Commerce has identified nine components that are needed for an effective ethics and compliance program:

1. A set of standards and procedures that guides employee conduct and helps stakeholders understand what to expect from a company's employees
2. A system that holds employees accountable for living up to the program's requirements
3. Clear communication of the program and policies to employees
4. Active monitoring of employee conduct
5. Encouraging employees to seek advice when they have ethics questions
6. Due diligence in hiring employees
7. Encouraging employees to follow the policies and guidelines
8. Management taking appropriate actions when the policies and guidelines are violated
9. Regularly evaluating the program's effectiveness[2]

The components reflect the four critical elements of an ethics and compliance program. First, a formal code must be written. Employees from various areas of the company should be involved in drafting the code. Second, the ethics and compliance program must be clearly communicated to employees and relevant stakeholders such as suppliers, customers, and investors. The communication effort should include management speeches, printed copies of the code—such as wallet-size cards—distributed, posting the code in key locations at the company, and posting the code on the company's web site and intranet. The communication should also include training to teach employees what the code is and how it should be used. Communication is a two-way street. Employees must be encouraged to report violations of the ethics and compliance code. One very useful reporting mechanism is the anonymous ethics hotline, which helps employees trust that retaliation is less likely.

Third, management must actively support the ethics and compliance program. Top management should speak in support of the program and serve as examples of it. Appointing a senior-level compliance officer is another means of demonstrating management commitment to an ethics and compliance program. It also helps if management institutes incentives for employee compliance. Fourth, there must be procedures in place for investigating complaints and punishing or correcting violators. Employees must believe something will be done if there is a violation. There should also be efforts to assess the effectiveness of the entire ethics and compliance process. This assessment can be built into the investigation and correction system.

Although it is important for stakeholders to know about the ethics and compliance program, the focus is on employees. Ideally an ethics and compliance program builds employee interest in ethics. Some employees may become ethical enthusiasts who inject the program into all their decisions. Others will become ethically committed, adopting the ethics and compliance program but still needing reinforcement to live the program. What a company wants to avoid are ethically unaware or ethically challenged employees. The ethically unaware do not know the program or have yet to embrace its standards. Employees need to become familiar with the program and appreciate why it is necessary. The ethically challenged have rejected the standards and place the company at risk. Such employees must be identified and removed from the organization or reformed in some manner. An organization cannot afford the liabilities created by ethically challenged employees.

CONCLUSION

Ethics does have links to business security. Ethical lapses can involve violating physical or information security guidelines. Ethics can be related to theft and substance abuse as well, two recognized areas covered by business security. Ethical misconduct places organizations at risk. Ethics and compliance programs can be used to reduce ethical lapses.

See also Competitive Intelligence; Crisis Management; Corruption as a Business Security Concern; Employee Background Screening and Drug Testing; Ethical Conduct Audit; Information Security; and Insider Threat.

NOTES

1. KPMG, "Integrity Survey 2005–2006," 2007, online at http://www.kpmg.com/aci/docs/surveys/050362_ForIntegritySurvNEW.pdf (accessed 13 Feb. 2007), pp. 1–10.

2. U.S. Department of Commerce, International Trade Administration, "The Business Ethics Program," 2004, online at http://www.ita.doc.gov/goodgovernance/adobe/bem_section_2/full_text_section_2.pdf (accessed 13 Feb. 2007), p. 53.

ETHICAL CONDUCT AUDIT

Robert C. Chandler

Most organizations have long acknowledged that business continuity planning is an essential priority in order to effectively anticipate, prevent, mitigate, and survive natural disasters, data loss, accidents, and deliberate malevolent acts. Many are only now discovering that *integrity continuity* planning is also a due diligence policy and business priority. Ethical issues must be on the strategic agenda. Such planning goes beyond compliance issues and reactive disciplinary policies to actually managing integrity. Integrity management should be a priority not only because it is legally required but also because it is the right thing to do.[1] Employees who know that certain workplace decisions, behaviors, and processes exist in an ethically judged context are more aware and motivated to act ethically. Those who perceive such activities as detached from an ethical context or who utilize an alternative (unethical) value paradigm (i.e., financial or perceived performance), are less aware of ethical implications and more motivated to act unethically.

In the current business ethics expectations and legal regulatory climate, executives and board members are obligated to establish programs to prevent and detect wrongdoing. This includes attempting in good faith to assure that a corporate information and reporting system exists as well as to actively assess, monitor, and manage the ethical conduct and compliance behavior decisions in their companies. A central part of this due diligence obligation is ensuring that a demonstrated effective ethics/compliance program is in place as well as systematically evaluating and assessing the status of compliance, ethical decision making, and lawful conduct among all of the employees and in all organizational structures, processes, and systems. Merely establishing a code of ethics or conduct—as well as having a compliance policy endorsed (while necessary)—is not sufficient to demonstrate its efficacy. The focus should not be on the (paper) policies (on the shelf) but rather on the people making decisions and engaging in activities that are overshadowed by possible ethical implications both inside and outside of the business offices. To truly measure the state of ethics or compliance requires systematically measuring the people, perceptions, behaviors, decisions, and processes in the context of their work activities using a reliable and valid method. This process is often described as an ethical conduct audit.

A shift from reviewing policies on the page to an ethical conduct audit of people, perceptions, and processes in "real life/real time" requires a change of focus. Periodic, thorough reviews of a policy guide, code, or manual are essential but inadequate in ascertaining an organization's current state of ethics or compliance. It is essential to move toward an assessment method that focuses more on what people are actually thinking and doing on a daily basis or when confronted with challenging situations rather than debating the policies to be printed in a book to sit on the shelf. This shift recognizes that codes of conduct truly "exist" in the minds and behaviors of those who make the decisions and engage in the business conduct where the risks of unethical conduct are present.

The more employees recognize a decision or behavior involving a question of ethics, the more conscious they are about acting ethically and the more likely they are to behave appropriately. Senior management must create a climate of integrity by setting the example and communicating the importance of professional integrity in the workplace. In addition, management can measure ethics and compliance by assessing their employees' perceptions, presumptions, and normative behaviors in important situations. The key goal should always be creating and sustaining an ongoing, consistent equilibrium of ethics and compliance. This process is sometimes called managing integrity.

Integrity management includes creating formal and informal systems to ensure that employees act in ways that ensure legal compliance as well as enact the corporate code of conduct goals consistently, professionally, and ethically. Integrity management is intertwined with managing the larger corporate culture and informal reward/motivation processes that impact employee decisions and behaviors in ways that transcend written policies. In many instances, major ethical scandals have occurred even in companies that have clear and explicit policies and codes of conduct. Obviously, more is involved than merely having policies in place to avoid, mitigate, and survive these risks. Every business must create structures and processes requiring all employees and managers to obey all legal requirements and regulations. Furthermore, common ethical and professional standards would obviously include assumptions (1) that decisions and behaviors are conducted honestly and (2) that employees and managers would never knowingly harm or do damage to fellow employees, stakeholders, customers, clients, or vendors by deception, misrepresentation, fraudulent report, coercion, conflict of interest, or other such acts.

Organizational integrity is the first line and fundamental strategic planning area to minimize the risks of major unethical scandals. Ethical misconduct disasters and scandals generate serious, costly risks to the continuity and survival of your business. Breakdowns of integrity collectively cost businesses billions of dollars in litigation, fraudulent financial acts, increased costs, fines, reputation and image damage, customer/client trust, lost sales, and recovery costs. Ethical failures can disrupt business operations just as significantly as can natural disasters, data loss, accidents, and deliberate malevolent acts. Such scandals incur enormous costs, impact your business, wound your reputation and brand, anger your stakeholders, and potentially land senior management in prison. No company is immune from these threats. Prudent businesses plan to manage integrity continuity by assessing their vulnerability to ethical disasters, taking proactive measures, and preparing their organizations to mitigate and survive should such scandals break.

Achieving consistent integrity is much more than simply ensuring legal and regulatory compliance. Proactive integrity continuity requires that a company have a fundamental strategic commitment to integrity, be aware of intrinsic risks, and build a culture of integrity in which its employees are likely to make ethical decisions and behaviors. Managing integrity depends on creating an ethical context in which employee decisions and behaviors are consistent with the mission critical goals of professional, ethical, and strategic processes. Managing integrity (as in managing people) involves managing employee's perceptions of situations and understanding of how they should act, behave, and make decisions in their various work situations.

RECOGNIZING THE RISK FOR INTEGRITY LAPSES

The sentiments of a top corporate executive's statement that an ethical scandal "couldn't happen to us" are intrinsically related to the aftermath statement

"I never thought this would happen to us." In reality, all of the common justifications for ignoring integrity continuity planning are based on unsubstantiated trust in unmanaged human nature and neglecting the systemic factors that give rise to ethical disasters. Managing integrity requires greater strategic planning and enactment than hiring "good, basically moral people." Even systematically hiring only employees with the highest levels of morals and ethics is no surefire method of preventing a major scandal. Neither does having a detailed written statement of ethics or specific documented policies guarantee preventing such disasters. (For example, the intent of the final sixty-five-page Enron corporate *Code of Ethics*, written in 2000, was to help guide employees for "conducting the business affairs . . . in accordance with all applicable laws and in a moral and honest manner."[2]) In addition, one cannot adequately avoid these scandals by delegating planning to subordinates.

Managing integrity continuity requires clarifying organizational standards and expectations, using such standards in the formation of formal and informal processes, being part of an active and ongoing training program to ensure employee alignment, meshing with the decision-making processes that occur at various levels and functions in the organization, and including vulnerable conduct in regular and periodic assessment of employee behavior.

All of these efforts should be considered at the highest levels of management. Integrity continuity planning must occur as part of the strategic planning process and be integrated with decisions on development, transformation, goal setting, prioritization, and regulatory compliance issues. Every organization is vulnerable to integrity disasters, and so such risks must be continually and proactively managed. A false sense of security prevents companies from creating a plan of action to follow should a disaster occur. Not all scandals are of the company's making; certain disgruntled antagonists will spread false rumors, generate slander, and distort the truth for their own self-interests. Nonetheless, the threat of such scandals and public disasters of all types, including ethical, necessitates strategic integrity continuity planning.

ETHICAL MISCONDUCT DISASTERS (EMDs)

An ethical misconduct disaster is a specific, unexpected, and nonroutine unethical event or series of unethical events that creates significant operational disruptions and threatens, or is perceived to threaten, an organization's continuity of operations.

While acknowledging no universally accepted definition of an EMD exists, I nevertheless argue that such scandals can negatively affect an organization, a major business unit, the reputation and image of a brand, as well as all stakeholders of the organization. An ethical misconduct disaster can also harm, perhaps severely, an organization's financial performance, impact employees, result in litigation and regulatory responses, and create a media circus capable of destroying the public's basic trust or belief in an organization. These scandals can threaten the continuity and very existence of the corporation (e.g., Enron).

Not every unethical decision that occurs is a crisis for the organization. In fact, businesses that effectively manage integrity can systemically absorb, react to, and appropriately adjust to most breakdowns in conduct or decisions. Poor choices happen all the time. The key is whether the organization has adequately planned to mitigate through prompt response, disciplinary actions, appropriate disclosure, communicating to the workforce, and public crisis management communication in order to manage these events so that they do not escalate into catastrophes. Misconduct—because of its severity, persistence, lack of quick and appropriate response; public scrutiny of the organization's mishandling of the event; or necessary involvement of legal or regulatory structures—may escalate to a level classified as a disaster for a business. Such an EMD goes beyond mere disruption of routine operations. It poses disastrous results that have potentially significant economic consequences or presents a threat to the survival of the organization.

Recent revelations about ethical misconduct scandals make the prospects of the "unthinkable ethical disaster" a realistic concern. Prudent strategic continuity planning must take into account the risks of EMDs along with other serious threats to business continuity. Recent headlines document the need for strategic integrity continuity planning. What do you think of when you hear the following names: Martha Stewart, Quest, Merrill Lynch, Tyco, Enron, WorldCom, Andersen, Sears, Mitsubishi Motors, United Way of America, Global Crossing, Adelphia, Smith Barney Citigroup, or the Roman Catholic Church? Senior executives are facing prison sentences as a result of some of these scandals. In a Sarbanes-Oxley world, what prudent executive would ignore the risks of ethical scandals? One study found that 62 percent of all companies experienced a "significant or major" integrity continuity disruption between 1986 and 1996.[3] The Categories of Ethical Misconduct Disasters box provides examples of the types of EMDs. Although predicting ethical scandals in American business is not

Categories of Ethical Misconduct Disasters (EMDs)

- Harassment and discrimination (e.g., ethnic, sexual)
- Criminal and illegal activities
- Financial improprieties (fraud and falsifying records)
- Customer/client deception
- Bribery and improper influence
- Failure to adhere to policy/regulations

an exact science, one *CFO.com* projection forecasts up to twenty "major" business ethical misconduct disasters every year.[4]

Ethical misconduct scandals can spring from any segment or level of a company's operations. The major categories of such disasters typically include instances of harassment or discrimination, criminal or illegal activities, financial improprieties, customer deception, bribery or improper influence, regulatory violations, corruption, and undisclosed conflict of interest.

These offenses can disrupt business operations; negatively affect performance; produce entangling regulatory scrutiny or litigation; create labor problems; damage reputation, image, and brand; and produce criminal charges against senior management or top executives. Sentencing guidelines, such as those of the *Uniform Federal Sentencing Guidelines for Organizations*, hold executives and senior management accountable by instructing judges to consider organizational efforts to plan, train, and implement policies to mitigate, enact full-disclosure efforts, and cooperate with authorities. Corporations are increasingly held accountable for their efforts to educate, train, and enable employees to act ethically, legally, and with integrity in the performance of their duties.

EXPECTATIONS FOR INTRINSIC ETHICAL ORIENTATIONS

Because ethical behavior is a growing concern across society in general, ethics issues are encroaching on the workplace on many different fronts. Times have changed since the days when one could uncritically assume that all employees are hired with a fundamental and rigid commitment to recognizing, understanding, and acting ethically in every possible situation. Furthermore, reward systems, unique temptations, or unseen pressures may affect the ethical decision

General Ethical Concern

According to a 2002 national study of 12,000 high school students:

- Seventy-four percent admitted cheating on an exam at least once in the past year.
- Thirty-eight percent admitted shoplifting at least once in the past year.
- Thirty-seven percent admitted that they would lie "in order to get a good job."

making of even moral individuals in certain situations. The General Ethical Concern box provides additional information about ethics in the United States.

The "inherent ethics" of the "good, moral people" that a company hires include the 76 percent of MBA graduates who reported their willingness to commit fraud to enhance profit reports to management, investors, and the public.[5] Less than 50 percent of employees believe their employers have high ethical integrity.[6] Thirty percent of all employees currently report that they "know or suspect ethical violations such as falsifying records, unfair treatment of employees, and lying to top management."[7] Specifically, 41 percent of employees in the private sector and 57 percent of employees in the public/government sector are aware of ethical misconduct or illegal activities.[8] Furthermore, 60 percent of employees state that they know of, but have not reported, instances of misconduct in their organizations. Most employees cite as reasons for not coming forward about ethical misconduct the lack of confidentiality policies, fear that existing policies won't protect them, and fear of "whistle-blower retaliation."

ETHICAL CONDUCT AUDITS

Senior management, particularly at the chief executive level, commonly ignores integrity continuity considerations. Research has found that 60 percent of chief executives and boards of directors failed to engage in integrity continuity planning discussions or to include such considerations in strategic planning.[9] Furthermore, 57 percent of companies "have never" incorporated integrity continuity planning at the strategic executive or board level.[10] More than half of all businesses fail to assess ethical misconduct risks or plan to ensure integrity continuity.[11] For example, 54 percent of companies do not have employee ethics compliance measurement in their performance appraisal criteria.[12] Another 56 percent have never conducted an ethical behavior compliance audit, and 23 percent have never engaged senior management in ethics/compliance training efforts.[13]

The U.S. Federal Sentencing Guidelines for Organizations (USFSGO) include expectations that organizations should actively communicate the standards and procedures for ethical conduct and appropriate compliance through instructional or informational dissemination or training efforts. An ethical conduct audit is an important tool for "consciousness raising," generating awareness, creating opportunities for instruction in ethics, compliance, and ethical decision making, and for demonstrating an organization's commitment to ethical conduct and full compliance. Furthermore, the USFSGO also articulates the expectation for demonstrated "monitoring and auditing of the organization's activities, and a mechanism for employees and other agents to report wrongdoing without fear of retribution."[14] Obviously, a systematic and thorough ethical conduct audit is one direct means of demonstrating a good-faith effort for complying with this USFSGO obligation. In fact, the ethical conduct audit may be a best practice for fulfilling this obligatory task.

It is imperative that companies carefully assess the integrity risks unique in their business and organizational culture, as well as performance reward systems, codes of ethics, compliance training, and employee development programs. The following basic questions can assist in analyzing a company's integrity, strengths, weaknesses, opportunities, and threats:

- On what criteria do you base confidence in your company's integrity continuity?
- Do all company personnel know how to act or behave ethically and appropriately in all situations and contexts?
- Do employees know the rules for each situation that may arise?
- How does the company know the employees have this information?

An ethical conduct audit systematically assesses the current state of ethical behavior and decision making in an organization. Ethical conduct audits utilize observational data collection, paper/pencil measurements of perceptions, interviews, focus groups, cultural analysis, as well as content analysis of documents, communication, and debriefing of decisions. The audit can be incorporated into ethics or compliance training initiatives, and some of the assessment data can be gleaned during such training exercises, simulations, and exercises. Although every ethical conduct audit is unique and designed to meet the intrinsic needs of the particular organization, its goals are almost universally shared by those who engage in the assessment process. The current state of ethical integrity in your organization can be assessed by looking at elements of behavior, perceptions, communication, and outcomes in the organization. A systematic audit of measurable dimensions of the organization is an inherent aspect of a complete ethical conduct audit. The ethical conduct audit box reviews its contributions to an organization.

The basic idea justifying active assessment of ethical conduct assumes that the existence of formal codes of ethical conduct alone is insufficient to prevent

Ethical Conduct Audit

An ethics conduct audit can do the following:

- Gather information.
- Establish reporting channels.
- Assess culture.
- Examine perceived reward system.
- Alert to "warning signs."
- Identify patterns of potential misconduct.

scandals or ensure integrity continuity. Active ethics efforts are the key for integrity continuity. A real-time assessment of what's going on in the minds and behaviors of your people determines how best to proceed to ensure ongoing ethical integrity or to anticipate and mitigate a major ethical misconduct disaster. Ethical concerns must be regarded similarly to other business disruption/resumption concerns. In most cases, ethical disasters involve employees who failed to follow their own internal corporate policies and guidelines. Rarely, if ever, does a scandal arise from a single individual acting independently from the larger system, culture, process, and reinforcement of expectation norms, all of which tend to facilitate, encourage, or reward ethical behavior.

These risks can be minimized by assessing employee conduct, integrity of the organizational culture (including measuring employees' knowledge and familiarity with polices, rules, and protocol); conducting effective, active ethical conduct training; and evaluating the effectiveness of ethical codes of conduct and training efforts. One approach that has been used with success to assess a company's strengths, weaknesses, opportunities, and threats is the ethical conduct audit.[15] Such an assessment can provide insight into both legal compliance behaviors as well as the ethical reasoning and decision making that are often difficult to see with unfocused or casual observation.

COMMITMENT TO INTEGRITY CONTINUITY

To survive crises of integrity, a company must fundamentally commit to the strategic goals of proactively managing integrity. Corporations should expect, reward, and encourage the ethical behavior of their employees. Postcrisis analysis of major ethical scandals has revealed that employees were frequently motivated by formal and informal reward systems and explicit and implicit expectations of management, or that they believed themselves to be acting consistently with the behavior of other employees in the organization. Far too many corporate scandals have occurred because the organization (culture, policies, or reward system) "enabled" the employee's unethical behavior.

Specifically, employees should not be required to "bend the rules" to successfully perform their job tasks. The consistent message (not mere words, but also reflected in reward structures) is that employees can and should act in ethical ways to complete their work. Managers should never, even inadvertently, reward an employee whose performance was achieved at the expense of integrity or ethical behaviors. Ethical decisions and behavior should be facilitated by culture, attitudes, and actions of the other employees and managers. Integrity is a process and way of working. Employees can be trained to make integrity a work habit. Ethical conduct is a dividend-paying, long-term investment, not an expense. Ethical misconduct is a fundamental breach of obligation to stakeholders.

FIVE KEY CONSIDERATIONS FOR YOUR ETHICAL CONDUCT AUDIT

Prudent executives can initiate at least five proactive considerations to move their organization toward integrity continuity goals and objectives.

Step 1: Establish Explicit Ethical Goals and Criteria

Have clear and explicit ethical goals and behavioral criteria. Every company should establish detailed codes of ethics and all applicable compliance expectations. Such standards can distinguish between legal and ethical conduct, but both cases warrant written definition of the organization's expectations upon individuals Criteria should include specific examples of common or routine situations, so that clear-cut "models" exemplify what decisions and behavior are expected of employees. In fact, the more such examples are descriptive of the types of choices and situations that employees might encounter, the more powerful such illustrations can serve as the basis for integrity ideals that are likely to be enacted. All of the ethical codes should be put in writing, distributed to, and reinforced with all employees.

Step 2: Demonstrate Commitment to Those Ethical Goals and Criteria

Although having a written code that explicitly defines ethical expectations is important, it is also crucial to demonstrate to your workforce that the organization takes seriously and is committed to expecting employees to meet and exceed such standards. Employees must easily see that any statements of ethical conduct expectations are not just "lip service." Executives must demonstrate top management's commitment to integrity as a strategic goal of the corporation. Designating a corporate ethics officer or creating an ethics management team helps to manage a strategic integrity plan and to signal commitment. Performance appraisal processes must tie rewards systems to indicators of integrity as well as to other measurements of productivity. It is important to reward integrity consistently, to make sure that these instances are known throughout the organization, and to have a clear and efficient disciplinary process for lapses of integrity.

Step 3: Communicate Ethical Expectations and Train Workforce to Enact

Create and disseminate (in multiple formats) integrity expectations and ethical criteria in such a way that everyone knows them. Every employee, manager, and executive in your company should participate in ethical training programs as part of the strategic commitment to integrity continuity management. Recognizing ethical dimensions of various situations, understanding the company's ethical expectations, applying ethical criteria in "complex" situations, carrying out ethical decision-making processes, implementing ethics in action, and legal compliance—such are the parts of an ongoing integrated training program. Given the recent scandals, it may also be prudent for every company to determine what ongoing ethical training initiatives are underway at its accounting firms, suppliers, vendors, distributors, or other "intertwined" entities.

Step 4: Assess and Monitor Employee Behavior and Decisions

Monitoring and auditing employee conduct (formal and informal) are essential to have a realistic picture of the types of behaviors and decisions that occur within your organization. Start with a comprehensive ethical conduct audit, and then review the various decision systems and critical points that may be vulnerable to lapses in integrity. Ethical training programs need to train employees to recognize and make ethical decisions. Review ongoing surveillance and collaborative participation efforts to ensure that all behaviors and decisions are being conducted ethically. Create and maintain whistle-blower channels, policies, and protections for those who report unethical conduct.

These analytical techniques and methods typically focus on areas such as the following:

- Analysis of evidence of proactive policies to facilitate and empower compliance and ethical conduct
- Data collection for any observed misconduct (reporting and processing procedural considerations)
- Systematic measurement of communication, culture, and individual perceptions of ethical issues
- Measuring perceptions and awareness of ethical issues among employees
- Evidence of key "warning signs" of potential underlying ethical issues
- Measuring ethical decision making capabilities among employees
- Evaluating reporting systems (confidential hotlines, etc.), ethics/compliance violations, and whistle-blower protections
- Perceptual personal commitments to integrity/professionalism among employees
- Believing that the ethics/compliance program contributes to better decision making
- Perceptions of ethical integrity by organizational constituents (stakeholders)
- Assessing the quality of ethical training and compliance programs.

Step 5: Maintain Ongoing Proactive Integrity Continuity Management

Managing integrity continuity requires ongoing commitment and proactive attention to maintain the processes and continuously achieve the ethical goals.

Proactive Integrity Management

Proactive integrity continuity management tactics follow:

- Set and maintain integrity goals at the strategic level.
- Demonstrate top management commitment to integrity.
- Monitor and audit conduct (formal and informal).
- Adjust policies and procedures based on ethical conduct audit findings.
- Tie performance rewards system to integrity conduct.
- Distribute written rules, policies, and procedures.
- Reinforce written rules, policies, and procedures.
- Train employees to recognize and make ethical decisions.
- Establish corporate ethics officer/team.
- Designate ethical compliance manager.
- Install surveillance and foster collaborative participation.
- Maintain whistle-blower channels and policies.
- Ensure supportive climate for ethical conduct.
- Reward acts of integrity and ethical decisions.
- Abide by and enforce disciplinary policy consistently and fairly.
- Offer organizational transformation (OT) training and development programs.
- Immediately respond to misconduct; follow procedures consistently and fairly.
- Continue ongoing assessment of ethical conduct and compliance.

Create and continue a supportive climate for ethical conduct by recognizing and rewarding acts of integrity and ethical decisions. Abide by and enforce disciplinary policies in consistent and fair ways. Conduct organizational transformation (OT) activities—training and development programs to build a corporate culture of integrity. Anticipate potential threats to integrity continuity. Develop and practice plans for reacting and responding to the discovery of unethical behavior. Have contingency plans for handling issues that might potentially become major scandals and disruptions to your ongoing operations. The Proactive Integrity Management box reviews the integrity continuity management tactics.

CONCLUSION

A comprehensive ethical conduct audit can provide a snapshot of the current state of ethics, ethical practices, compliance, and integrity across your organization and among your workers. The focus of an ethical conduct audit is to assess the current state of ethics as practiced by employees in many different business contexts, and it includes issues such as accounting integrity as well as discrimination, bribery, deception, customer fraud, cheating, theft, and interacting with others in a fair and appropriate manner. The Overview of Conducting an Ethical Audit box provides a quick checklist.

An ethical conduct audit reviews the various decision systems and critical points at which you may be vulnerable to lapses in integrity. It also identifies "hot spot" issues that need to be addressed in subsequent compliance programs and training efforts. If your company has declared a "zero tolerance" policy for ethics and legal/regulatory compliance, then a comprehensive ethical conduct audit can verify that those goals are shared (buy in) and adhered to (compliance), and that the processes for responding to violations of the policies are consistent with the mandates of the policies themselves.

Overview of Conducting an Ethical Audit

1. Determine Specific Audit Objectives

   Examples include:

   - Ascertain the current state of compliance.
   - Ascertain the level of ethical decision-making skills.
   - Identify potential warning signs.
   - Spot-check (randomly sampled) ethical compliance.
   - Measure degree of awareness of ethics policies.
   - Validate reporting and whistle-blowing channels functionality.
   - Gather attitudes and predispositions toward ethical issues.
   - Verify the effectiveness of ethical training programs.
   - Discover which ethical issues are the most salient or likely to create a full-blown ethical conduct disaster.
   - Assess the quality of ethical compliance programs.

2. Create/Adapt Audit Tools (Multiple Measures) to Gather Data

   Tools can include:

   - Content analysis techniques
   - Questionnaires and surveys
   - Confidential 360 measurements
   - Psychometric (in-depth) assessment
   - Observation
   - Interviews

(continued)

- Focus groups
- Outcome (post-facto) reviews
- Self-report methods
- Simulations and exercises
- Training follow-up evaluation
- Culture studies

3. Analyze the Data

   Analytical techniques and methods are typically focused on areas such as the following:

   - Analysis of evidence of proactive policies to facilitate and empower compliance and ethical conduct
   - Data collection for any observed misconduct (reporting and processing procedural considerations)
   - Systematic measurement of communication, culture, and individual perceptions of ethical issues
   - Measuring perceptions and awareness of ethical issues among employees
   - Evidence of key "warning signs" of potential underlying ethical issues
   - Measuring ethical decision-making capabilities among employees
   - Evaluating reporting systems (confidential hotlines, etc.), ethics/compliance violations, whistle-blower protections
   - Perceptual personal commitments to integrity/professionalism among employees
   - Believing that the ethics/compliance program contributes to better decision making
   - Perceptions of ethical integrity by organizational constituents (stakeholders)

4. Draw Conclusions and Action Items

   Review the various decision systems and critical points where you may be vulnerable to lapses in integrity. Ethical training programs should go beyond reviews of policies and rules (and disciplinary actions) to train employees to recognize and make ethical decisions. Review ongoing surveillance and collaborative participation efforts to ensure that all behaviors and decisions

(continued)

are being conducted ethically. Create and maintain whistle-blower channels, policies, and protections for those who report unethical conduct.

5. Close the Loop: Proactive Ethical Development and Training Efforts

   The conclusion phase of an ethical conduct audit is just the foundation for moving forward toward sustaining a culture of integrity within your organization. These findings are the springboard for the next steps of compliance program enhancements, as well as development and training efforts. Ethical training programs should go beyond reviews of policies and rules (and disciplinary actions) to train employees to recognize and make ethical decisions. Review ongoing surveillance and collaborative participation efforts to ensure that all behaviors and decisions are being conducted ethically. Create and maintain whistle-blower channels, policies, and protections for those who report unethical conduct.

See also Business Continuity; Corruption as a Business Security Concern; and Ethics as a Business Security Concern.

NOTES

1. Debre Thorne Clair, O. C. Ferrell, and John P. Fraedrich, *Integrity Management: A Guide to Managing Legal and Ethical Issues in the Workplace* (Tampa, FL: University of Tampa Press, 1998).
2. *Enron Code of Ethics*, Enron Corporation, 2000, p. 2.
3. Jonathon A. Gottlieb and Jyostna Sanzgiri, "Towards an Ethical Dimension of Decision Making in Organizations," *Journal of Business Ethics*, 15 (1996), 1275–1285.
4. Stephen Taub, "Crisis of Ethics: Ethics Officers Predict a New Wave of Corporate Scandals," *CFO.COM*, 19 June 2002, online at http://www.cfo.com/article.cfm/3005220?f=search (accessed 20 Sept. 2002).
5. Cathy Lazere, "Ethically Challenged: Teaching Ethics Is Required but Schools Have Wide Latitude in How They Do It," *CFO Magazine*, April 1997.
6. Walker Information and Hudson Institute, *Workforce 2020* (Indianapolis, IN: Walker Information and Hudson Institute, 1999).
7. Walker Information and Hudson Institute, *Workforce 2020*..
8. "Integrity and Ethics in Public Administration: Polls and Surveys," *Public Management*, Oct. 1998 (Washington, DC: Public Management, 1998), pp. 3–4.

9. Taub, "Crisis of Ethics."

10. Taub, "Crisis of Ethics."

11. Robert C. Chandler and J. D. Wallace, "Brief Results of the Pepperdine University Ethical Misconduct Disaster Recovery Preparedness Survey," *Disaster Recovery Journal*, 14, 3 (2001), 21–22.

12. Taub, "Crisis of Ethics."

13. Chandler and Wallace, "Brief Results of the Pepperdine University Ethical Misconduct Disaster Recovery Preparedness Survey," p. 22.

14. U.S. Federal Sentencing Guidelines for Organizations, "Framework for Assessing Ethics/Compliance Programs," http://www.ethicaledge.com/assessment%20framework.htm (accessed 15 Feb. 2007).

15. Robert C. Chandler, "Managing Ethical and Regulatory Compliance Contingencies: Planning and Training Guidelines," *Contingency Planning and Management 2000 Proceedings* (Flemington, NJ: Witter Publishing, 2000), pp. 6–7.

EMPLOYEE THEFT AND FRAUD

W. Timothy Coombs

The fraud by Tyco and Enron executives made news headlines around the world. But beneath these extreme cases lie a number of smaller incidents that amount to a very large problem for organizations. The billions of dollars lost each year due to employee theft and fraud affect both small and large organizations alike. Many of the other entries have indirectly touched on this problem and suggested solutions to it. This entry explores the problems of employee theft and fraud and reviews key ideas for prevention.

THEFT

Employee theft is a significant problem in the retail industry. It is the primary source of inventory "shrinkage" in retail, accounting for 47 percent of all retail loss. The loss from employee theft was over $14 billion in 2004 and has been increasing since 2002.[1] Over 30 percent of all employees admit to stealing from an employer, and an estimated 75 percent of employee theft goes undetected.[2]

But employee theft is not limited to the retail industry. Other industries, such as pharmaceuticals, experience employee theft through in-transit/cargo theft. Cargo theft, the weakest link in a global supply chain, costs organizations between $10 billion and $14 billion annually. Government estimates claim that 80 percent of all in-transit/cargo theft is connected to employees (insiders).[3] Employee theft can also include goods and office equipment. Efforts to prevent employee theft begin with employee background screening. Also required are basic physical security and cargo security measures as efforts to combat employee theft, including access control, CCTV monitoring, and security guards. Another preventative measure is to conduct routine but unannounced inventory audits to identify whether equipment is missing. Oddly, inspecting the garbage is a preventative measure; some employees hide items in the garbage and return after closing hours to retrieve them. Finally, management must model good behavior and not condone minor thefts.

FRAUD

Employee fraud is a rather broad topic that includes misappropriation of assets (theft and misuse of organizational assets), fraudulent financial statements, and corruption. Fraudulent acts share the same four characteristics: they (1) are clandestine, (2) violate an organization's fiduciary responsibilities, (3) are purposeful, and (4) drain resources from an organization. Employees know they are doing something wrong, and trying to hide it makes the task of catching them that much more challenging. The warning signs include working late, not wanting to leave work, change in lifestyle, sudden wealth, and erratic behavior. A number of other factors could lead to these same warning signs, so don't jump to conclusions. Comprehensive security is the best defense and solution to employee fraud.

Misappropriation of assets includes organizational assets, such as the previous discussion of retail and cargo theft, and money. Over 80 percent of all misappropriations are financial. Employees use a variety of means for taking money, including skimming (taking money from a client and not reporting it), stealing money before depositing it in a bank, and creating fake billing receipts. Fraudulent financial statements are types of creative bookkeeping (e.g., improper asset valuation and fictitious revenues) used for embezzlement. Authorizing third-party financial audits and having multiple people involved in distributing funds are ways to check for fraudulent financial statements.

Corruption includes bribery, conflict of interests, and illegal gratuities.[4] See the entries Corruption as a Business Security Concern and Ethics as a Business Security Concern for more details on corruption and how to combat it.

CONCLUSION

We like to think the best of the people with whom we work or who work for us. However, it can be costly to be naïve about employee theft and fraud. As the Insider Threat entry noted, your employees are a source of risk. They have the access to and knowledge about your organization to steal a variety of organizational assets, including equipment and money, or to commit fraud. Managers are wise to combine careful employee screening with physical and information security that watches insiders as well as outsiders. Making it difficult for employees to steal or commit fraud coupled with a culture that promotes integrity helps management reduce a very serious source of financial loss for its organization.

See also Biometrics; Corruption as a Business Security Concern; Culture of Integrity; Employee Background Screening and Drug Testing; Ethics as a Business Security Concern; Integrating Physical and Information Security; Physical Security; Radio Frequency Identity; Security Guards/Officers; Supply Chain Security; and Video Surveillance.

NOTES

1. ADT Security Services, Inc., "2004 National Retail Survey," 2005, online at http://www.adt.com/wps/wcm/resources/file/eb05060b959d9e6/NRSS_05_fact_sheet.pdf (accessed 19 June 2007).

2. John Case, *How to Identify Dishonesty Within Your Business: The 97 Early Warning Signs of Internal Theft* (Del Mar, CA: Business Security Publications, 2004).

3. "Tenth Pharmaceutical Industry Conference Report," 2002, online at http://www.dediversions.usdoj.gov/mtgs/pharm_indutry/10th_pharm.htm (accessed 19 June 2007).

4. "2006 ACFE Report to the Nation on Occupational Fraud & Abuse," 2006, online at http://www.acfe.com/documents/2006-rttn.pdf (accessed 19 June 2007).

REPUTATION MANAGEMENT

W. Timothy Coombs

A number of the entries have mentioned the terms *reputation* and *reputation management*. So what is the connection between reputation and business security? The concern is that security breaches, if they become a public incident or crisis, cause damage to an organization's reputation. This entry explains what a reputation is and how it is created, why a reputation is important to an organization, and methods for assessing the reputation of an organization as part of a preparedness program.

REPUTATION: DEFINITION

An organization's reputation is an aggregate evaluation stakeholders make about how well an organization is meeting stakeholder expectations based on its past behaviors. Put another way, a reputation is an evaluation of an organization based on stakeholder perceptions. As evaluations, reputations are favorable or unfavorable. Because reputations are evaluative, some point of comparison is required. Stakeholders compare what they know about an organization to some standard to determine whether an organization meets their expectations for how an organization should behave. Because reputations are based in large part on stakeholders' evaluations, a failure to meet expectations, an expectation gap, is problematic for organizations.

Stakeholders are any group that can affect or be affected by the behavior of an organization. Common stakeholders include customers, suppliers, investors and financial analysts, community members, employees, the news media, government agents, and activist groups. Reputations are perceptual and may not reflect reality, which means some organizations might have unwarranted favorable or unfavorable reputations. One reason management needs to track a reputation is to make sure it fairly represents the organization.

REPUTATION: THE BENEFITS

Reputations are widely recognized as a valuable, intangible asset. Intangible means you cannot touch it like you could a physical asset. However, you can measure a reputation and assess its value. When managers were asked to rate thirteen intangible resources, reputation was ranked number one. Some of the proven benefits associated with a favorable reputation are generating investment interest, improving financial performance, attracting top employee talent, increasing the return on assets, creating a competitive advantage, and garnering positive comments from financial analysts. Favorable reputations provide a sustained competitive advantage by allowing an organization to differentiate itself from its competitors. Some experts estimate that up to 63 percent of a company's market value is attributable to its reputation.[1] Clearly, favorable reputations provide organizations with a number of rewards. Unfavorable reputations produce the opposite effect and serve to hold an organization back.

REPUTATION: FORMATION AND DAMAGE FROM CRISES

A reputation develops through the information stakeholders collect about the organization. Stakeholders receive information through interactions with an organization, mediated reports about an organization (including the news media and advertising), and secondhand information from other people (e.g., word of mouth and weblogs). Through interactions, stakeholders can see for themselves whether the organization's actions match their expectations for the organization. Does the product perform as advertised? Is the customer service department helpful? Is the organization meeting projected financial goals?

Most of the information stakeholders collect about organizations is derived from reports about how an organization acts rather than through direct contact with the organization. Because the dominant source of information about organizations is the news media, media coverage is an important feature of reputation management efforts. Most stakeholders cannot see for themselves whether a company treats its workers fairly, has tight security, or uses only suppliers who do not exploit child labor. But the news media and other people can provide this information. The news media can report on the nature of an organization's suppliers, whereas employees might tell others about their experiences directly or through a weblog. Secondhand information from social media on the Internet, such as weblogs or blogs, is critical for some situations.

Consider how stakeholders find out about security breaches. Those who could be affected by the security should be notified directly (interaction with the organization). Others learn about such situations through news reports or online sources such as blogs, online news stories, or postings to discussion boards. As a personal example of how this works, I read a news story about my mortgage company losing a tape of account holder information before the company contacted me. I felt the mortgage company was slow in acting. Later, I learned of a breach involving my credit card company in a letter from the company and before the story broke in the news media. The same direct and indirect methods hold true for other crises. Stakeholders experience the crisis directly if they are victims or potential victims who have been warned about a crisis. Most stakeholders learn about a crisis through the news media or secondhand information. Most people know about the Exxon *Valdez* oil spill, although very few saw it with their own eyes. Secondhand information can be an important source of information when that source is respected or trusted by stakeholders.

Kryptonite, the bicycle lock makers, and Edelman Public Relations' fake supportive blogs for Wal-Mart are examples of crises that transpired primarily online rather than in the news media. Owners of Kryptonite locks revealed online how these locks could be picked with a pen casing and even posted videos showing that it really could be done. These sources were trusted because they owned the locks and wanted to warn others about the problem. Edelman received intense online criticism when it was revealed it had paid the couple blogging about visiting Wal-Marts while on a trip across the United States. Although the news media eventually covered these crises, the online environment was their primary arena. Stakeholders commonly learn about reputation threats, such as crises, through the news media and secondhand information. In fact, experts find that the news media and online sources serve to magnify crises and incidents, making the threat to reputation even greater.

Security breaches and other crises threaten to damage reputations because a catastrophe gives people reasons to think badly of the organization. Again, the news media and the Internet play a critical role. Most stakeholders learn about a crisis from news reports. In a smaller number of crises, stakeholders find out about crises through online social media. The exceptions would be victims or potential victims who are more likely to experience the crisis or to be informed directly by the organization about the crisis. If a reputation shifts from favorable to unfavorable, stakeholders can change how they interact with an organization. Clearly the benefits of a favorable reputation noted earlier may be lost. Furthermore, stakeholders may sever ties to the organization and/or spread negative word of mouth about it.

Corporate leaders are very concerned about threats to reputations, including crises. Business executives rate reputation risk as their most serious problem and rank it well ahead of terrorism and natural disasters. Business executives believe reputation threats are on the rise and nearly nine in ten executives say the trend is for increasing reputation threats.[2] Clearly, a reputation threat is a problem, given the many benefits derived from a reputation. The concern is compounded by the fact that business executives estimate it takes three to three and a half years to recover from an event that damages a reputation. Business leaders maintain it is far easier to build a reputation than to recover from a damaged reputation. Many of the preventive measures discussed in this book, including business security, help to reduce the number of reputation-damaging events a company may face.

REPUTATION: MEASUREMENT

If management is concerned about its reputation and potential damage to it, it must be able to evaluate its reputation. Evaluation allows management to track the reputation and determine whether it is changing over time or how much of an impact a crisis has had on it. This section discusses four commonly used reputation measures: *Fortune*'s "Most Admired Companies," the Reputation Quotient, the Media Reputation Index, and the RepTrak^{TM}.

The best known of the reputation measures is *Fortune*'s annual list of the "Most Admired Companies." The Most Admired list is based on eight key attributes of a reputation: (1) innovativeness, (2) ability to attract, develop, and keep talented people, (3) quality of management, (4) quality of products and services, (5) value as a long-term investment, (6) financial soundness, (7) community and environmental responsibility, and (8) use of corporate assets. *Fortune* developed these eight attributes through a series of interviews with executives and analysts to determine what makes a company admirable. The *Fortune* results are based on surveys completed by senior executives, outside directors, and financial security analysts. The focus of the Most Admired reputation is on the financial performance and the potential of a company.

Harris Interactive and the Reputation Institute developed the Reputation Quotient. Well-known reputation expert Charles Fombrun, who runs the Reputation Institute, took the lead in developing this measure. The Reputation Quotient examines twenty reputation attributes that are divided into six "drivers" of reputation: (1) products and services, (2) financial performance, (3) workplace environment, (4) social responsibility, (5) vision and leadership, and (6) emotional appeal. The Reputation Quotient is based on surveys from business leaders.

The Media Reputation Index is closely related to the Reputation Quotient. Originally developed by Delahye Media Link, the Media Reputation Index evaluates media coverage of a company. The rationale is that the news media help to shape a company's reputation. The Media Reputation Index uses the six drivers from the Reputation Quotient to categorize the media coverage. The stories are then coded as to being positive or negative for a particular dimension. The scores are added together to form the Media Reputation Index.

In 2006, the Reputation Institute launched a new reputation measurement tool called the RepTrak^{TM} Model. This model reflects how reputations have evolved since the Reputation Quotient was developed in 1997. The RepTrak Model has twenty-three key performance indicators grouped around seven core dimensions: (1) products and services, (2) innovation, (3) workplace, (4) governance, (5) citizenship, (6) leadership, and (7) performance. Much like the Most Admired list, the Reputation Quotient and related measures have a strong financial element. All four measures weight financial performance heavily when evaluating a reputation.

Cees van Riel, a leader in reputation management in Europe, reviewed a number of reputation measures including the Most Admired list and the Reputation Quotient. Van Riel found trust to be one of the key elements shared by the many measures.[3] The Guidance Appendix includes a measure that any company can use to assess stakeholder trust in the company. The Organizational Reputation Scale offers a simple and useful measure of a company's reputation.

NEXT EVOLUTION IN REPUTATION: CORPORATE SOCIAL RESPONSIBILITY

It is important to recognize the financial bias in popularly used reputation measures. Business executives and many reputation experts believe that reputations are evolving away from financial performance and toward social performance. Social performance is an indicator of a company's corporate social responsibility. Corporate social responsibility recognizes that corporations have responsibilities beyond just earning money for investors. Corporations are obligated to the many other stakeholders whose lives they can impact. In the broadest sense, corporate social responsibility is the recognition that organizations have responsibilities beyond shareholders, including social concerns. Corporations must consider how their operations impact society. These social impacts are broad, including such issues as poverty, environmental damage, sustainability, human rights, treatment of workers, disease control/eradication, and treatment of indigenous peoples. Organizations seek to be a net contributor to society. A working definition of corporate social responsibility is the management of actions designed to affect an organization's impacts on society. Corporate social responsibility becomes the actions a company takes to further the social good.

Both business executives and reputation experts believe corporate social responsibility has had a growing influence on reputations. Over 55 percent of business executives surveyed felt that corporate social responsibility contributes "a lot" to the company's reputation.[4] Corporate social responsibility, not financial performance, seems to be the most important driver of corporate reputation. If corporate social responsibility is rising in importance, the four most commonly used measures of reputation are becoming outdated. Each touches on corporate social responsibility in some way but as a minor, rather than a featured, component.

An alternative measure of reputation that does focus on corporate social responsibility is the Best Corporate Citizen assessment developed by *Business Ethics* magazine, with Sandra Waddock and Samuel Graves of Boston College providing the statistical analysis framework. The Best Corporate Citizen scores are based on five social dimensions developed by KLD Research & Analytics: (1) environment, which includes programs from pollution reduction recycling to energy savings, as well as negative measures such as level of pollutants and EPA citations; (2) community relations, which includes philanthropy, creating foundations, community service, scholarships, and employee involvement; (3) employee relations, which includes wages, benefits paid, family-friendly policies and employee empowerment; (4) diversity, which includes minority and women workers and managers, diversity programs, any EEOC complaints, and lawsuits; and (5) customer relations, which includes quality of management programs, quality awards, customer satisfaction measures, and lawsuits.

CONCLUSION

Reputation as a concept continues to grow in importance for companies. Companies work hard to build their reputations and work just as hard to protect them. Business security, emergency management, and crisis management can all help a company to avoid incidents and crises that can damage a reputation. The Crisis Communication: External and Internal entry specifically discusses how communication can be used to help repair a reputation after a crisis hits. Because their work is connected to reputation, people in business security should be aware of this concept and its effects on an organization.

See also Corruption as a Business Security Concern; Crisis Communication: External and Internal; Crisis Management; Ethics as a Business Security Concern; and Ethical Conduct Audit.

NOTES

1. Weber Shadwick, "Safeguarding Reputation," online at http://www.webershandwick.com/pub/content/reputation.pdf (accessed 24 Feb. 2007), p. 2; and Hill and Knowlton, "Corporate Reputation Watch," online at http://www2.hillandknowlton.com/crw/home.asp (accessed 23 Feb. 2007).

2. Aon, “Dominant Risk Issues,” 2006, online at http://www.aon.com/uk/en/about/Press_Office/biennial_2005 /biennial_2.jsp (accessed 24 Feb. 2007).

3. Guido Berens and Cees B. M. van Riel, “Corporate Associations in the Academic Literature: Three Main Streams of Thought in the Reputation Management Literature,” *Corporate Reputation Review*, 7 (2004), 161–178.

4. Shadwick, “Safeguarding Reputation,” p. 2.

PSI Handbook of Business Security

PSI Handbook of Business Security

VOLUME TWO

SECURING PEOPLE AND PROCESSES

EDITED BY W. TIMOTHY COOMBS

Praeger Security International
Westport, Connecticut • London

Library of Congress Cataloging-in-Publication Data

PSI handbook of business security / edited by W. Timothy Coombs.
2 v. ; cm.
Includes bibliographical references and index.
Contents: v. 1. Securing the enterprise—v. 2. Securing people and processes.
ISBN 978-0-275-99394-8 (set : alk. paper) — ISBN 978-0-275-99395-5 (vol. 1 : alk. paper) — ISBN 978-0-275-99396-2 (vol. 2 : alk. paper)
1. Industries—Security measures. I. Coombs, W. Timothy. II. Title: Handbook of business security.
HV8290.P77 2008
658.4'7—dc22 2007040469

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2007040469

ISBN-13: 978-0-275-99394-8 (set)
978-0-275-99395-5 (vol. 1)
978-0-275-99396-2 (vol. 2)

First published in 2008

Praeger Security International, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the United States of America

The paper used in this book complies with the
Permanent Paper Standard issued by the National
Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

CONTENTS

VOLUME 1: SECURING THE ENTERPRISE

INFORMATION (CYBER) PROTECTION

TERRORISM AS A BUSINESS SECURITY AND SAFETY CONCERN

GENERAL SAFETY CONCERNS

UNCOMMON BUSINESS SECURITY CONCERNS

VOLUME 2: SECURING PEOPLE AND PROCESSES

PHYSICAL PROTECTION

SECURITY ON A GLOBAL SCALE

ENHANCING THE HUMAN SIDE OF SECURITY AND SAFETY

PREFACE

In general, security means freedom from risk, fear, doubt, or anxiety. For organizations, business security comprises the measures taken to protect people, data, physical assets, and financial and other assets. These measures help to create a safe workplace and to reduce risks. Business security further seeks to combat the various security risks faced by organizations. When these risks become a reality, people and organizations suffer. Examples include workplace violence, terror attacks, computer hacking/data loss, disruption of the supply chain, and top management engaged in illegal acts. Moreover, these "problems" draw intense coverage from the news media, which are drawn to singular, negative events. Negative publicity resulting from incidences that might have been avoided further harms an organization by damaging its reputation, which is a valuable, if intangible, resource. Business security clearly involves high stakes.

When most people think about business security, a security guard at a front desk or gate comes to mind. Others may think of the password they have to enter when they use their computers at work. Business security is much more extensive and involved than these two common reference points. The diversity of business security is a reflection of the multitude of risks that organizations face. The security guard and the computer password represent two broad areas of business security—physical security and information security—but many more areas of concern exist. There is obviously a concern for people at a location (employees, vendors, and visitors), the grounds, the building itself, and the materials in the building. Yet business security extends outside of the facility to people and businesses located near the facility, cyberspace, vendors and others in the supply chain, and so forth. These two volumes try to capture the range and complexity of business security.

The objectives of the *PSI Handbook of Business Security* are twofold. The primary objective is to create a reference tool for people involved in business security. The entries and resources identify key security concerns and provide guidance on how to handle them. This work thus serves as a resource for anyone looking to improve security in an organization.

The secondary objective is to raise people's awareness of their role in security. If employees fail to commit to business security, the organization is at risk. What are the odds that new hires, such as fresh college graduates, know much about security or appreciate its value? Does your orientation program properly educate them on physical and information security? Do these new people read and commit themselves to abiding by the security policies in the employee handbook? Do your long-time employees understand and appreciate their role in business security? Anyone who reads the *PSI Handbook of Business Security* should realize that every employee plays an active role in keeping an organization secure.

Business security is complex and multifaceted. This set is comprised of two volumes that explore this diverse area. Volume 1 focuses on information security, terrorism, and topics related to business security that often are not included in discussions of business security. Volume 2 focuses on physical security, the growing global concerns of business security, and the role people play in making business security a success.

I am grateful to the many experts who took time from their busy lives to contribute to this project. They embraced it and realized the importance of sharing what they know with others to help improve business security. Hopefully, readers will benefit from the information compiled in these two volumes and use it to make their workplaces safer.

Volume 1: *Securing the Enterprise*

The workplace is very different than it was just ten years ago. Computers and the Internet have become common business tools. The tragic events of 9/11 still resonate in organizations, as terrorism remains a concern. Corporate misdeeds from Enron, Tyco, and others have resulted in new regulations, creating renewed interest in business ethics. This changing workplace environment requires revisions in how we approach business security. The entries in Volume 1: *Securing the Enterprise* reflect this evolving workplace.

Volume 1 begins with the Information (Cyber) Protection section. While computers and the Internet increase business productivity, they also create enormous security risks. Protecting data and access to a computer system must be a priority for all organizations and a concern that all employees share. The entries reflect the range of issues and concerns that emerge as information security grows in importance. This section starts with a general discussion of information security and then moves to core concepts in information security:

- Security models
- Security documentation
- Security policies and standards

These core concepts are followed by a collection of additional information security concerns including the security threats and ways to protect Internet and e-mail use, portable device use, insider threat, and social engineering.

Terrorism is a reality that organizations face all around the globe and is broader than most people might think. The Terrorism as a Business Security and Safety Concern section begins with an analysis of terrorism including the global locations at greatest risk. The entry Ecoterrorism reflects the broad nature of terrorism. The breadth and scope of terrorism have implications for business security. Organizations anywhere, for example, might have to deal with environmental groups targeting a facility. Another feature of this section is its consideration of special terrorist risks for agriculture (Agroterrorism, Strategic Partnership Program Agroterrorism, and Food Security) and the chemical industry (Terrorism and Chemical Facilities). Both industries are prime terror targets and need to address terror concerns as part of business security.

The General Safety Concerns section relates to the connections between security and safety. This section examines the role of business security in protecting people and things both inside and outside of the organization. Efforts to protect employees and others in and around an organization must address the concerns generated by significant negative events such as disasters, crises, emergencies, and business disruptions. These negative events are often interconnected and can be threats inside and outside of the organization. The entries cover these important areas:

- Emergency preparedness and response component
- Disaster recovery management
- Business continuity
- Crisis management

Preparations for these negative events are a key to safety, and security can contribute significantly to these efforts. These entries concentrate on crisis management and emergency management because of the strong focus these two processes have on protecting people.

Finally the Uncommon Business Security Concerns section reflects the growing concern over ethics in organizations (Ethics as a Business Security Concern and Ethical Conduct Audit) and the issues of corruption (Corruption as a Business Security Concern) that arise as organizations compete in a global business environment. Ethical and corruption issues do relate to business security. Competitive intelligence is included because organizations can step over the ethical line when seeking competitive intelligence and should know how to make it more difficult for others to collect intelligence on them. The final entry, Reputation Management, is included because many other entries note the negative effect that security lapses can have on an organization's reputation. This entry explains why damage to a reputation is such a strong business concern.

Volume 2: *Securing People and Processes*

As the workplace changes, the core need for physical protection remains but its nature changes as well. The Physical Protection section contains a variety of entries related to protecting people, equipment, and buildings. The main topics include the following:

- Security guards/officers
- Workplace violence
- Employee background screening and drug testing
- Video surveillance
- Radio frequency identity
- Biometrics
- Shelter-in-place
- Evacuation

The last entry in this section explains how physical and information security are beginning to merge and what the benefits of that synergy are.

The Security on a Global Scale section recognizes the unique security demands of global organizations. The Terrorism entries touched on the subject, but this section's entries look at the problems and possible security solutions when an organization is connected to various locations around the world. The topics include the following:

- Pandemics
- Outsourcing
- Supply chain security
- Travel overseas
- Corporate or industrial espionage

A theme that echoes throughout this introduction and collection is the importance of all employees in security. The entries in the Enhancing the Human Side of Security and Safety section concentrate on how to work with employees to embrace programs that will make a more secure workplace. The focus is on how to integrate new programs into an organization by avoiding the silo thinking that prevents integration, winning acceptance, and integrating the new programs into the organizational culture. The entries also provide tips on how to create teams and the value of exercises and training.

Volume 2 also includes the Guidance Appendix, Resource Appendix, Documents Appendix, and Glossary. The Guidance Appendix provides "how-to" advice on a number of the topics in the two volumes; whereas the Resource Appendix lists books, magazines, and web sites that can provide additional information on a variety of the entries. The Document Appendix offers a collection of government documents that are useful reference tools for those interested in business security. Last, the Glossary provides an extensive list of terms related to business security. It is a useful tool for clarifying the meaning of terms or concepts and learning the diverse vocabulary of business security.

Business security is a complex topic that involves a wide range of activities and preventative measures. Hopefully the *PSI Handbook of Business Security* does justice to the complicated nature of the topic. Many departments in an organization have a role to play in business security. These two volumes illustrate how the various elements of business security in an organization must work in concert and include all employees in that effort. This project will be a success if people use the ideas in this book to improve security in their organizations.

ACKNOWLEDGMENTS

I would like to thank the many attendees and presenters at CPM West that I have talked to and heard over the years. Your ideas about and insights into business security helped to guide the development of this project. I would also like to thank Jeff Olson at Praeger Publishers, Greenwood Publishing Group, for his dedicated attention to and editing of this project.

PHYSICAL PROTECTION

The most visible part of business security is physical security. People can see security guards, fences, gates, and video cameras. This section examines a range of concerns related to physical security. It includes procedures and methods for improving physical security for people, facilities, and products.

PHYSICAL SECURITY

W. Timothy Coombs

Any organization that has a building or an office has a need for physical security. Many employees think of physical security when they hear the term *security* because it is usually the most visible aspect of business security. We see security guards, card readers, gates, and closed circuit television cameras (CCTV). (The term *CCTV* is used generically for all camera systems, including the newer digital systems.) Physical security includes efforts to monitor and control the facility's exterior and interior perimeters. Its scope includes mail service security, lock and key controls, and perimeter and interior alarms. Physical security is a layering process of overlapping activities designed to keep bad people out and to keep your people, information, and physical assets safe.

AREAS AND SECURITY MEASURES

Physical security begins at the site perimeter. There need to be physical barriers to prevent access to your facility, even if it is an office building rather than a production or transportation facility. A fence with detection systems, electronic gates with card readers, other barriers, and security officer checkpoints can separate your facility from the outside world. The guards and electronic gates help to monitor who is actually inside your perimeter, such as employees, delivery personnel, vendors, or other visitors. Facilities that are likely terrorist targets may want to consider examining all vehicles entering the parking area, especially underground parking. Security officers should be looking for any indications the vehicle may contain explosives. Also consider rearranging physical barriers periodically to change the traffic flow into a facility. Predictability is a friend to a possible intruder.

Make sure the perimeter is easily visible with plenty of lighting and removal of anything that could block sight lines such as vegetation or signs. Use technology to enhance coverage of the perimeter. Install motion detectors, electronic beams, CCTV cameras, and microwave perimeter intrusion systems. Be certain all of your security officers are trained in the use of the systems and the desired security protocols.

The main entrance to the building should have high-security locks and doors, CCTV cameras, and security officers. The entrance can also be equipped with two-way voice communication and biometric card readers. The two-way communication allows outsiders contact with people inside without a person gaining access, and the biometric cards help ensure only the proper people get inside. Refer to the Biometrics entry for more details on that system. Secondary personnel entrances should be secured as well with high-security locks, strong door closers, CCTV cameras, card readers with biometrics, and motion-sensitive lighting.

Shipping and receiving is a third means of entry into a building. Security officers and CCTV cameras should be positioned there. It is important that drivers do not leave their designated areas and that all shipments are verified. To check cargo, the shipping and receiving area should have X-ray equipment, radio frequency identification (RFID) equipment, and bar code scanners. Your people need to verify that the proper cargo is being delivered and nothing “extra” is in the shipment.

Inside a facility, there is the need to monitor interior doorways and elevators. Card readers and biometrics should be used to limit access to different areas of the building. Not all employees require access to all areas of a facility. In high-security areas, make sure only authorized personnel have access. Support the access control system with CCTV cameras to monitor who is actually entering and leaving, and reinforce the door jambs and locks to prevent people from forcing their way into a secure area. One of the areas you must treat as high security is the security/life safety control room, which contains your CCTV monitors and recorders, alarm panel, lighting control, fire suppression systems, HVAC controls, and the communication system. Compromise of any of these systems means a facility is at risk. Make sure the doors have reinforced jambs and there are biometric card scanners.

Finally, make certain to store, lock, and inventory keys, access cards, uniforms, badges, and vehicles. Any of these assets can be used to compromise an organization's security by providing a means of access to a facility.

PHYSICAL SECURITY IS EVERYONE'S CONCERN

Your employees should not think that physical security is taken care of by the security staff. Reinforce that everyone has a role to play in security. Television news reports have demonstrated how easy it is for a well-dressed person to enter an office and take a laptop computer. All employees should know the need for badge and area challenges. Employees should confront people without badges or who are not in a designated area. Challenge involves asking the persons who they are and why they are there. Security should be contacted if the wrong answers are given. Employees also need to make sure all windows and doors are properly

Suspicious Activity

This information comes from the Department of Homeland Security's "Report Suspicious Behavior and Activity" brochure.

- *Surveillance.* Someone is recording or monitoring activities at your facility. People are seen with cameras, taking notes, or using binoculars.
- *Deploying assets.* There are abandoned vehicles, packages, or luggage near a facility.
- *Suspicious people.* There are people who do not seem to belong in the workplace, in the office, or near the facility.
- *Suspicious questioning.* Someone is trying to get information about your facility over the phone, in person, or through e-mail.
- *Tests of security.* There are actions taken to test the physical security of the facility.
- *Acquiring supplies.* There are attempts to buy the ingredients for explosives.
- *Dry runs.* Someone observes what appear to be preparations for an attack such as mapping routes or timing traffic lights.[1]

closed and locked. Unlocked windows and doors provide easy egress for would-be intruders. Be sure to report any broken windows, doors, or locks as soon as they are spotted. Train employees on what constitutes suspicious behavior so that they can identify and report those behaviors. Key points for suspicious activities include entrances, loading docks, parking areas, and garages. See the Suspicious Activity box for additional information.

EVOLUTION OF PHYSICAL SECURITY

A trend in physical security is its growing use of technology and integration with IT security. This entry has mentioned biometrics, CCTV, and microwave perimeter intrusion systems—all technology-driven features of physical security. Although attentive and well-trained security officers are still the heart of physical security, their efforts are supplemented and enhanced by technology. The entry Integrating Physical and Information Security elaborates on this topic.

CONCLUSION

You must assume that certain people out there would like to access your facility for a variety of nefarious activities ranging from theft to terrorism. Physical security is a critical defense to keep these people out of your facility or from inflicting injury on your personnel. Security is a process of integrating various protective systems and devices to create a web of safety around a facility and its personnel. Your employees must realize that physical security, like information security, is everyone's responsibility and that they have a role to play in keeping a facility or building safe.

See also Biometrics; Integrating Physical and Information Security; Supply Chain Security; Terrorism; Terrorism and Chemical Facilities; and Travel Overseas.

NOTE

1. U.S. Department of Homeland Security, "Protect Your Workplace," online at http://www.us-cert.gov/reading_room/brochure_securityguidance.pdf (accessed 14 March 2007).

SECURITY GUARDS/OFFICERS

W. Timothy Coombs

Organizations often have a legal duty to provide security to employees, customers, and visitors. Security guards have a variety of responsibilities including perimeter security, heating and cooling systems, communication, alarm systems, receiving visitors and providing information, and responding in emergency situations. Beyond keeping people and facilities safe, security guards are essential elements in business continuity, emergency management, and crisis management. The job can be both routine and dangerous. Hiring security guards is an important consideration for management. This entry reviews key issues related to employing security guards.

GENERAL TYPES OF SECURITY GUARD

Because organizations vary in terms of what they need from a security guard, there are different types of security guards. Some organizations simply need a friendly deterrent. Their security guard is a visual deterrent to shoplifters and possible miscreants. People expect the security guard to be friendly and helpful. The guard provides information, directions, or even calls when a patron needs assistance with automobile problems in the parking lot.

A second type of security guard is one to prevent employee theft. The friendly but firm security officer is more of an authority figure, and this seriousness must be reflected in the security officer's looks and attitude. The security guard is approachable but serious, primarily there to prevent loss. The final type of security guard is one that watches over the movement of money. These armed guards should convey a simple message: stay away. The organization must be sure the security officer's characteristics match the its needs.

Certain qualities are required of all security guards. Security guards should look neat, clean, and project a professional image. They must have uniforms that are clean and be neatly groomed. They need to understand that confrontation is to be resolved, not escalated. Security guards should be trained in methods for handling and de-escalating conflicts. If security guards are to carry a weapon, they require the necessary registration and training.[1]

HIRING SECURITY GUARDS

Thorough background checks are required before hiring security guards. Refer to the entry Employee Background Screening and Drug Testing for additional information on this topic. Management must be certain the person is actually qualified for the position, including a clean criminal record. Hiring a security guard with a criminal record is a recipe for a negligent hiring suit. Check all references, previous work history, and credentials. You must be sure the person can do the job, has the proper attitude for the specific position, and has the necessary credentials. Organizations must also have an official policy on the use of force and weapons. An organization risks liability if such policies are lacking and someone is injured due to a use of force or weapons.

Organizations have three basic hiring options: full-time officers, contracted officers, and part-time officers drawn from law enforcement personnel or firefighters who are moonlighting. Full-time officers will have a familiarity with the facility, and management can be certain of training and screening. The disadvantages are the costs associated with training and supervising full-time officers. It falls to the organization to ensure officers are trained to current standards. Using contracted officers moves the training costs and responsibility to the security company. The disadvantage is that the officer may be less committed to the organization, and management cannot be certain of credentials. Management must carefully evaluate the quality of the officers being provided by a vendor.

The third option is law enforcement people and firefighters who are moonlighting. These well-trained professionals may have insights about community threats the organization is not yet aware of. There are cost savings, but the issues of integration and commitment remain a concern. An organization cannot rely solely on part-time security. There need to be full-time security guards who serve as team trainers, supervisors, and leaders. Full-time security officers also make sure there is integration between the organization and the part-time security force. A key point of that integration is informing the part-time officers about the unique security needs of the organization, such as hazardous waste issues.[2]

CONCLUSION

Whatever mix of security guards an organization uses, management must be diligent in vetting all security officers. Security guards should reduce, not increase, an organization's liability. Careful evaluation and training of all security personnel will ensure this is the case.

See also Employee Background Screening and Drug Testing; Integrating Physical and Information Security; and Physical Security.

NOTES

1. David C. Tryon, "Limiting Liability: Guarding Against Legal Problems," online at https://www.schinnerer.com/risk_mgmt/security/pdfs/stnd0901.pdf (accessed 15 March 2007).

2. Robert E. Uhorchak and Stanley N. Parker, "Solving the Security/Safety Staffing Paradox, *Risk Management Magazine*, Sept. 2005, pp. 60–61.

WORKPLACE VIOLENCE PREVENTION AND POLICIES

Geary Sikich

It seems that the subject of workplace violence has been overshadowed in recent years by the events of September 11, 2001, the war in Iraq, Iranian nuclear aspirations, global warming, and a host of other issues. However, the "Survey of Workplace Violence Prevention, 2005," published by the Bureau of Labor Statistics (BLS), U.S. Department of Labor, for the National Institute for Occupational Safety and Health (NIOSH), Centers for Disease Control and Prevention, reports:

> Nearly 5% of the 7.1 million private industry business establishments in the United States had an incident of workplace violence within the 12 months prior to completing a new survey on workplace violence prevention. Although about a third of these establishments reported that the incident had a negative impact on their workforce, the great majority of these establishments did not change their workplace violence prevention procedures after the incident; almost 9% of these establishments had no program or policy addressing workplace violence.[1]

The Survey of Workplace Violence Prevention looked at the prevalence of security features, the risks facing employees, employer policies and training, and related topics associated with maintaining a safe work environment.

Over 128 million workers were employed at the 7.4 million establishments represented by the survey. In an average week in U.S. workplaces, one employee is killed and at least 25 are seriously injured in violent assaults by current or former coworkers.

Many of the incidences of workplace violence can be prevented. According to *USA TODAY*:

> In nearly eight of 10 cases, killers left behind clear warning signs—sometimes showing guns to co-workers, threatening their bosses or talking about attacking. But in the majority of cases, employers ignored, downplayed or misjudged the threat, according to a *USA TODAY* analysis of 224 instances of fatal workplace violence.[2]

It is interesting that less than 20 percent of the companies targeted in such attacks took any action to enhance security or put internal prevention steps in place.

A PRESCRIPTION FOR PREVENTION

Imagine the following scenario unfolding.

> Your phone rings—4:00 p.m. Friday.
> A simple phone call and all your weekend plans are canceled.
> 4:15 p.m.: Another phone call. An employee you thought you knew well has just redefined your weekend.
> The phone rings again. You now have a full-scale crisis on your hands. The employee you thought to be so stable will become a quick study for you and your staff.
> Another phone call. You can't believe the amount of emotion, confusion, and misinformation generated by the incident.

And this is just the beginning.

When I first began creating and conducting workshops on workplace violence in the 1990s, the phenomenon of violence in the workplace was not new; it was and still is potentially one of the most serious problems facing organizations and individuals. And, we continue to turn a blind eye to a critical aspect of the problem—nonreporting of events. In the 1990s, not much literature existed on the subject of workplace violence. Today, while more literature exists, managers and human resource departments have yet to come up with answers. Outside consultants help to develop and implement appropriate prevention policies and programs, but the incidence of violence continues unabated.

The Bureau of Labor Statistics (BLS) entered into an interagency agreement with NIOSH to conduct a survey, mentioned above, of U.S. employers regarding their policies and training on workplace violence prevention. The survey defined workplace violence as violent acts directed toward a person at work or on duty (i.e., physical assaults, threats of assault, harassment, intimidation, or bullying). Workplace violence was classified as four types of situations:

- *Criminal:* When the perpetrator has no legitimate relationship to the business or its employees and is usually committing a crime in conjunction with the violence (e.g., robbery, shoplifting, or trespassing)
- *Customer or Client:* When the perpetrator has a legitimate relationship with the business and becomes violent while being served by the business (e.g., customers, clients, patients, students, inmates, or any other group to which the business provides services)
- *Coworker:* When the perpetrator who attacks or threatens another employee is an employee, past employee, or contractor who works as a temporary employee of the business
- *Domestic violence:* When the perpetrator, who has no legitimate relationship to the business but has a personal relationship with the intended victim, threatens or assaults the intended victim at the workplace (e.g., family member, boyfriend, or girlfriend)[3]

Nokia's CEO, Jorma Ollila, seems to sum it up quite well in an excerpt reported by the *Moscow Times* in 2005: "[P]eople are more concerned about individual rights than taking responsibility for their actions and trying to have a positive influence on society."[4]

Why do we consistently fail to identify risks or teach employees how to defuse workplace situations indicating that an attack may be imminent? One reason is "culture"; we as a society frequently fail to react when we are scared. Think about how many times you have had a premonition and did not take extra precautions to enhance your safety and security. Organizations consistently fail, even after an event such as a firing or disciplinary hearing that could trigger an attack. Indeed, *USA TODAY*'s findings are supported by other research. "In more than 100 instances that I studied, in every case there was evidence to suggest this person was hurting and had a potential for aggression," said Jeff Landreth, a senior vice president at New York-based Guardsmark, a security services company. "We found the threats were ignored."[5]

Here are some of the key elements for an effective workplace violence prevention program:

- *Establish a threat management policy.* Make sure that it is adhered to and that regular reviews are conducted in order to assure that it works.
- *Conduct regular threat analysis reviews.* Periodic threat analysis can facilitate early recognition and possibly defuse a situation just waiting to erupt.
- *Develop a threat management team.* Include management, staff, human resources, and external entities that can bring expertise to bear on the threat analysis reviews.
- *Communicate effectively with all employees.* Communication is such a key element and so mismanaged. Tremendous resources are available to organizations to help them with the communication process. Listen to what is being said—then hear what is being said.
- *Develop procedures that provide early warning and clear instructions on what to do if an incident occurs.* I have developed and facilitated the use of a simple system called *IPAC*™, which has been proven effective in a number of settings, from heavy industry to financial services. The acronym stands for *I*dentify, *P*rotect, *A*lert, *C*ommunicate.[6]
- *Develop a system that provides continual assessment of and feedback on actual or potential situations.* Active analysis can be effectively implemented to provide information from many sources that creates a mosaic resulting in a clearer picture of a situation.
- *Develop training programs for employees to reduce the potential for violence in the workplace and elsewhere.* Well-informed and -educated personnel can be your best deterrent to workplace violence.
- *Develop wellness programs including stress management.* Ensure that the programs are implemented, as these can also defuse situations before they become a crisis.

- *Develop an employee assistance program.* Utilize third-party expertise and ensure that there are no negative ramifications for using the program. Again, implement the program to make sure that employees at all levels are aware and can take advantage of it.
- *Ensure fair compensation and promotional practices.* Involve human resources and other applicable elements of your organization in the process to ensure fair treatment of employees. Stress that employees are personally responsible for their actions too.
- *Provide reasonable sick leave and vacation policies.* This can be as creative as your human resource department wishes. You may also benefit from involving legal specialists early on to ensure that appropriate standards of care are addressed.
- *Improve termination policies and procedures.* Termination policies should be clearly defined and uniformly enforced.

PROGRAMS AND POLICIES

Over 70 percent of workplaces in the United States do not have a formal policy addressing workplace violence. In establishments that reported having a workplace violence program or policy, private industry most frequently reported addressing coworker violence (82 percent). Customer or client violence was the next most frequent subject of private industry policies or programs (71 percent), followed by criminal violence (53 percent) and domestic violence (44 percent). While addressing customer/client and coworker workplace violence the most, state governments dealt with domestic violence (66 percent) more than criminal violence (53 percent), whereas equal numbers of local governments addressed domestic violence and criminal violence (47 percent).[7]

Although most occurrences of workplace violence center on a single employee, companies involved in restructuring, layoffs, and mass termination should pay close attention. How an organization handles the restructuring, layoffs, and/or termination can create a significant potential for acts of violence. When employees are being terminated for any reason, management should demonstrate caring and a sincere interest in the future welfare of these individuals.

Employers may consider providing employees being terminated with such assistance as outplacement services, psychological counseling, severance benefits, skills development, and training and educational assistance. However, it is important to emphasize that outplacement services and any other assistance should be provided off-site, so that terminated employees are not encouraged to return to their former place of employment.

Although there are often displays of certain characteristics and behavior prior to a violent act occurring, management generally is not trained to detect such warning signs. Missing these apparently obvious signals from the discontented employee often leads to self-blame after the fact. A training program to help personnel identify warning signs should be developed and implemented. Certain characteristics and behavior constitute a profile that personifies the likely candidates and should trigger a red flag:

- Male between thirty-five and fifty-five years old
- Midlife transition, dissatisfied with life
- Loner without a true support system
- Low self-esteem
- Generally works in jobs with high turnover
- History of being disgruntled during employment
- Tends to project one's own shortcomings onto others
- History of intimidating coworkers and supervisors
- Feels persecuted and views efforts to help with suspicion
- Watches others for violations and may keep records
- Interested in weapons; may be a collector or marksman
- Probably does not have a police record

Take potential warning signs seriously. When a person displays several characteristics or behaviors outlined here, an employer should pay attention. Management, at all levels, that lacks the necessary experience and expertise to handle this type of potentially explosive situation should rely on appropriate outside resources—for example, specialized psychological counseling or extra security measures—on a temporary or even permanent basis.

Organizations must have these resources identified and in place in order to preempt a potentially devastating situation effectively. There is no time to plan or seek these resources as an incident is unfolding.

DESIGNING A PLAN

Taking the time to develop a detailed plan for what to do in a crisis is essential for getting an organization back on its feet in a more expedient and effective manner. The plan should establish important guidelines for accomplishing critical tasks efficiently during a time of crisis. For violence in the workplace, these tasks may include the following:

- Notification and communication procedures
- Humanitarian assistance for injured employees
- Humanitarian assistance for victims' families
- Real-time counseling of distressed employees
- Organizing professional counseling services
- Emergency repair and damage control activities
- Modified work schedules and temporary services

- Communicating with community and clients
- Media management

Specific tasks involved in developing and implementing the plan include building a threat management team, creating appropriate procedures for implementing the plan, preparing contingency scenarios, training personnel, and conducting crisis simulation drills and exercises.

Clearly, having a well-conceived program consisting of the policy, the plan, implementing procedures, and a trained staff to implement it will place your company in the best position to protect its assets (employees and property) from the potentially devastating effects of an incidence of workplace violence.

Here are some sample workplace violence prevention program and policy documents that may prove useful for your program development.

SAMPLE WORKPLACE VIOLENCE PREVENTION PROGRAM

POLICY STATEMENT
(EFFECTIVE DATE FOR PROGRAM)

Our establishment, [*Employer Name*], is concerned and committed to our employees, and their safety and health. We refuse to tolerate violence in the workplace and will make every effort to prevent violent incidents from occurring by implementing a Workplace Violence Prevention (WPVP) Program. We will provide adequate authority and budgetary resources to responsible parties so that our goals and responsibilities can be met.

All managers and supervisors are responsible for implementing and maintaining our WPVP Program. We encourage employee participation in designing and implementing our program. We require prompt and accurate reporting of all violent incidents whether or not physical injury has occurred. We will not discriminate against victims of workplace violence.

A copy of this Policy Statement and our WPVP Program is readily available to all employees from each manager and supervisor.

Our program ensures that all employees, including supervisors and managers, adhere to work practices that are designed to make the workplace more secure, and do not engage in verbal threats or physical actions that create a security hazard for others in the workplace.

All employees, including managers and supervisors, are responsible for using safe work practices, for following all directives, policies, and procedures, and for assisting in maintaining a safe and secure work environment.

The management of our establishment is responsible for ensuring that all safety and health policies and procedures involving workplace security are clearly communicated and understood by all employees. Managers and supervisors are expected to enforce the rules fairly and uniformly.

Our program will be reviewed and updated annually.

WORKPLACE VIOLENCE PREVENTION PROGRAM

THREAT ASSESSMENT TEAM

A Threat Assessment Team will be established, and part of its duties will be to assess the vulnerability to workplace violence at our establishment and reach agreement on preventive actions to be taken. They will be responsible for auditing our overall Workplace Violence Program.

The Threat Assessment Team will consist of:

Name: Title: Phone:
Name: Title: Phone:
Name: Title: Phone:
Name: Title: Phone:

The team will develop employee training programs in violence prevention and planning for responding to acts of violence, and will communicate this plan internally to all employees. The Threat Assessment Team will begin its work by reviewing previous incidents of violence at our workplace. It will analyze and review existing records identifying patterns that may indicate causes and severity of assault incidents and identify changes necessary to correct these hazards. These records include but are not limited to OSHA 200 logs, past incident reports, medical records, insurance records, workers' compensation records, police reports, accident

(continued)

investigations, training records, grievances, minutes of meetings, and so on. The team will communicate with similar local businesses and trade associates concerning their experiences with workplace violence.

Additionally, the team will inspect the workplace and evaluate the work tasks of all employees to determine the presence of hazards, conditions, operations, and other situations that might place our workers at risk of occupational assault incidents. Employees will be surveyed to identify the potential for violent incidents and to identify or confirm the need for improved security measures. These surveys shall be reviewed, updated, and distributed as needed or at least once within a two-year period. Periodic inspections to identify and evaluate workplace security hazards and threats of workplace violence will be performed by the following representatives of the Assessment Team, in the following areas of our workplace:

Representative: Area:
Representative: Area:
Representative: Area:

Periodic inspections will be performed according to the following schedule: frequency (daily, weekly, monthly, etc.).

SAMPLE SELF-INSPECTION SECURITY CHECKLIST

Facility:
Inspector:
Date of Inspection

1. Security Control Plan: Yes No

If yes, does it contain:
(A) Policy statement Yes No
(B) Review of employee incident exposure Yes No
(C) Methods of control Yes No
If yes, does it include:
Engineering Yes No
Work practice Yes No
Training Yes No
Reporting procedures Yes No

Record keeping Yes No
Counseling Yes No

(D) Evaluation of incidents Yes No
(E) Floor plan Yes No
(F) Protection of assets Yes No
(G) Computer security Yes No
(H) Plan accessible to all employees Yes No
(I) Plan reviewed and updated annually Yes No
(J) Plan reviewed and updated when tasks added or changed Yes No

2. **Policy Statement by Employer** Yes No

3. **Work Areas Evaluated by Employer** Yes No

If yes, how often?

4. **Engineering Controls** Yes No

If yes, does it include:

(A) Mirrors to see around corners and in blind spots Yes No
(B) Landscaping to provide unobstructed view of the workplace Yes No
(C) “Fishbowl effect” to allow unobstructed view of the interior Yes No
(D) Limiting the posting of sale signs on windows Yes No
(E) Adequate lighting in and around the workplace Yes No
(F) Parking lot well lighted Yes No
(G) Door control(s) Yes No
(H) Panic button(s) Yes No
(I) Door detector(s) Yes No
(J) Closed circuit TV Yes No
(K) Stationary metal detector Yes No
(L) Sound detection Yes No
(M) Intrusion detection system Yes No
(N) Intrusion panel Yes No
(O) Monitor(s) Yes No
(P) Videotape recorder Yes No
(Q) Switcher Yes No
(R) Handheld metal detector Yes No
(S) Handheld video camera Yes No
(T) Personnel traps (“Sally traps”) Yes No
(U) Other Yes No

5. **Structural Modifications** (Plexiglas, glass guard, wire glass, partitions, etc.) Yes No

If yes, comment:

(continued)

6. **Security Guards**

(A) If yes, are there an appropriate number for the site? Yes No

(B) Are they knowledgeable of the company WPVP policy? Yes No

(C) Indicate if they are:

Contract guards (1) Yes No

In-house employees (2) Yes No

(D) At entrance(s) Yes No

(E) Building patrol Yes No

(F) Guards provided with communication? Yes No

If yes, indicate what type:

(G) Guards receive training on workplace violence situations? Yes No

Comments:

7. **Work Practice Controls** Yes No

If yes, indicate:

(A) Desks clear of objects that may become missiles Yes No

(B) Unobstructed office exits Yes No

(C) Vacant (bare) cubicles available Yes No

(D) Reception area available Yes No

(E) Visitor(s)/client(s) sign in/out Yes No

(F) Visitor(s)/client(s) escorted Yes No

(G) Barriers to separate clients from work area Yes No

(H) One entrance used Yes No

(I) Separate interview area(s) Yes No

(J) ID badges used Yes No

(K) Emergency numbers posted by telephones Yes No

(L) Internal phone system Yes No

If yes, indicate:

Does it use 120 VAC building lines? Yes No

Does it use phone lines? Yes No

(M) Internal procedures for conflict (problem) situations Yes No

(N) Procedures for Employee Dismissal Yes No

(O) Limit Spouse and family visits to designated areas Yes No

(P) Key control procedures Yes No

(Q) Access control to the workplace Yes No

(R) Objects that may become missiles removed from area Yes No

(S) Parking prohibited in fire zones	Yes	No
Other:		
7a. **Off-Premises Work Practice Controls**		
(For staff who work away from fixed workplace, such as social services, real estate, utilities, policy/fire/sanitation, taxi/limo, construction, sales/delivery, messengers, and others)		
(A) Trained in hazardous situation avoidance	Yes	No
(B) Briefed about areas where they work	Yes	No
(C) Have reviewed past incidents by type and area	Yes	No
(D) Know directions and routes for day's schedule	Yes	No
(E) Previewed client/case histories	Yes	No
(F) Left an itinerary with contact information	Yes	No
(G) Have periodic check-in procedures	Yes	No
(H) After hours contact procedures	Yes	No
(I) Partnering arrangements if deemed necessary	Yes	No
(J) Know how to control/defuse potentially violent situations	Yes	No
(K) Supplied with personal alarm/cellular phone/radio	Yes	No
(L) Limit visible clues of carrying money/valuables	Yes	No
(M) Carry forms to record incidents by area	Yes	No
(N) Know procedures if involved in incident (see also Training section)	Yes	No
8. **Training Conducted**	Yes	No
If yes, is it:		
(A) Prior to initial assignment	Yes	No
(B) At least annually thereafter	Yes	No
(C) Does it include:		
Components of security control plan	Yes	No
Engineering and workplace controls instituted at workplace	Yes	No
Techniques to use in potentially volatile situations	Yes	No
How to anticipate/read behavior	Yes	No
Procedures to follow after an incident	Yes	No
Periodic refresher for on-site procedures	Yes	No
Recognizing abuse/paraphernalia	Yes	No
Opportunity for Q and A with instructor	Yes	No
On hazards unique to job tasks	Yes	No
9. **Written Training Records Kept**	Yes	No

(continued)

10. **Are Incidents Reported?** Yes No
If yes, are they:
(A) Reported in written form Yes No
(B) First report of injury form (if employee loses time) Yes No

11. **Incidents Evaluated** Yes No
(A) EAP counseling offered Yes No
(B) Other action (reporting requirements, suggestions, reporting to local authorities, etc.) Yes No
(C) Are steps taken to prevent recurrence? Yes No

12. **Floor Plans Posted Showing Exits, Entrances, Location of Security Equipment, Etc.** Yes No
If yes, does it:
(A) Include an emergency action plan, evacuation plan, and/or a disaster contingency plan? Yes No

13. **Do Employees Feel Safe?** Yes No
(A) Have employees been surveyed to find out their concerns? Yes No
(B) Has the employer utilized the crime prevention services and/or lectures provided by the local or state police? Yes No

Comments:

General Comments/Recommendations:

SAMPLE INCIDENT REPORT FORM

1. VICTIM'S NAME:
JOB TITLE:
2. VICTIM'S ADDRESS:
3. HOME PHONE NUMBER:
WORK PHONE NUMBER:
4. EMPLOYER'S NAME AND ADDRESS:
5. DEPARTMENT/SECTION:
6. VICTIM'S SOCIAL SECURITY NUMBER:
7. INCIDENT DATE:
8. INCIDENT TIME:
9. INCIDENT LOCATION:
10. WORK LOCATION (if different):

11. TYPE OF INCIDENT (circle one):
Assault, Robbery, Harassment, Disorderly Conduct, Sex Offense, Other (Please Specify)

12. WERE YOU INJURED: (circle): Yes No
If yes, please specify your injuries and the location of any treatment:

13. DID POLICE RESPOND TO INCIDENT: Yes No
14. WHAT POLICE DEPARTMENT:
15. POLICE REPORT FILED: Yes No
REPORT NUMBER:
16. WAS YOUR SUPERVISOR NOTIFIED: Yes No
17. SUPERVISOR'S NAME:
18. WAS THE LOCAL UNION/EMPLOYEE REPRESENTATIVE NOTIFIED: Yes No
Whom should be notified?
19. WAS ANY ACTION TAKEN BY EMPLOYER (specify):
20. ASSAILANT/PERPETRATOR (circle one):
Intruder, Customer, Patient, Resident, Client, Visitor, Student, Coworker, Former Employee, Supervisor, Family/Friend, Other (specify):
21. ASSAILANT/PERPETRATOR—NAME/ADDRESS/AGE (if known):
22. PLEASE BRIEFLY DESCRIBE THE INCIDENT:
23. INCIDENT DISPOSITION (circle all that apply):
No Action Taken, Arrest, Warning, Suspension, Reprimand, Other (specify):
24. DID THE INCIDENT INVOLVE A WEAPON: Yes No
(Please Specify)
25. DID YOU LOSE ANY WORK DAYS:
(Please Specify)
26. WERE YOU SINGLED OUT OR WAS THE VIOLENCE DIRECTED AT MORE THAN ONE INDIVIDUAL:
27. WERE YOU ALONE WHEN THE INCIDENT OCCURRED:
28. DID YOU HAVE ANY REASON TO BELIEVE THAT AN INCIDENT MIGHT OCCUR: Yes No
Why:
29. HAS THIS TYPE OR SIMILAR INCIDENT(S) HAPPENED TO YOU OR YOUR COWORKERS: Yes No
(Please Specify)

(continued)

30. HAVE YOU HAD ANY COUNSELING OR SUPPORT SINCE THE INCIDENT: Yes No
(Please Specify)

31. WHAT DO YOU FEEL CAN BE DONE IN THE FUTURE TO AVOID SUCH AN INCIDENT:

32. WAS THIS ASSAILANT INVOLVED IN PREVIOUS INCIDENTS:

33. ARE THERE ANY MEASURES IN PLACE TO PREVENT SIMILAR INCIDENTS: Yes No
(Please Specify):

34. HAS CORRECTIVE ACTION BEEN TAKEN:
(Please Specify):

35. COMMENTS:

SAMPLE EMPLOYEE SECURITY SURVEY

This survey will help detect security problems in your building or at an alternate work site.

Please fill out this form, get your coworkers to fill it out, and review it to see where the potential for major security problems lie.

NAME:

WORK LOCATION:
(IN BUILDING OR ALTERNATE WORK SITE)

Do either of these two conditions exist in your building or at your alternate work site?

Work alone during working hours

No notification given to anyone when you finish work

Are these conditions a problem? If so when, please describe. (For example, Mondays, evening, Daylight Savings Time)

Do you have any of the following complaints (that may be associated with causing an unsafe work site)?

(Check All That Apply)

Does your workplace have a written policy to follow for addressing general problems?

Does your workplace have a written policy on how to handle a violent client?

When and how to request the assistance of a coworker

When and how to request the assistance of police
What to do about a verbal threat
What to do about a threat of violence
What to do about harassment
Working alone
Alarm system(s)
Security in and out of building
Security in parking lot
Have you been assaulted by a coworker?

To your knowledge, have incidents of violence ever occurred between your coworkers?

Are violence-related incidents worse during shift work, on the road, or in other situations?
(Please Specify)

Where in the building or work site would a violence-related incident be most likely to occur (specify)?

Have you ever noticed a situation that could lead to a violent incident?

Have you missed work because of a potential violent act(s) committed during your course of employment?

Do you receive workplace violence–related training or assistance of any kind?

Has anything happened recently at your work site that could have led to violence?

Can you comment about the situation?

Has the number of violent clients increased?

CONCLUSION

Many employers believe it can’t happen to them. New policies to prevent violence were adopted after a fatal 1998 shooting at the state transportation department office in Greeley, Colorado. Accountant Robert “Scott” Helfer, 50, had a history of arguments with supervisors. As a meeting was held to discuss employee complaints against him, he shot and killed equal employment representative

Sharlene Nail and wounded Karla Harding, a regional transportation director. Helfer was later shot and killed by a state trooper in the parking lot.

Having effective policies and an aggressive program to track behavior if anything seems abnormal is essential. You never want to have to utter the following words to a reporter: "My mistake was I never saw him as a time bomb that would explode."

See also Contributors to Workplace Aggression; Employee Background Screening and Drug Testing; and Workplace Aggression.

NOTES

[1] Bureau of Labor Statistics (BLS), U.S. Department of Labor, for the National Institute for Occupational Safety and Health (NIOSH), Centers for Disease Control and Prevention; "Survey of Workplace Violence Prevention, 2005," 2005, online at http://www.bls.gov/iif/osh_wpvs.htm (accessed 23 April 2007).

[2] Stephanie Armour, "Managers Not Prepared for Workplace Violence," *USA TODAY*, 15 July 2004, online at http://www.usatoday.com/money/workplace/2004-07-15-workplace-violence2_x.htm (accessed 23 April 2007).

[3] Bureau of Labor Statistics, "Survey of Workplace Violence Prevention, 2005."

[4] Matti Huuhtanen, "Nokia CEO Laments 'An Era of Selfishness,' " *Moscow Times*, 25 Jan. 2007, online at www.themoscowtimes.com/stories/2005/01/25/259.html (accessed 23 April 2007).

[5] Armour, "Managers Not Prepared for Workplace Violence."

[6] Geary W. Sikich, *Integrated Business Continuity: Maintaining Resilience in Times of Uncertainty* (Tulsa, OK: PennWell Publishing, 2003).

[7] Bureau of Labor Statistics, "Survey of Workplace Violence Prevention, 2005."

WORKPLACE AGGRESSION

W. Timothy Coombs

Workplace aggression, an important concern in the workplace, can be defined as "efforts by individuals to harm others with whom they work, or have worked, or the organization in which they are currently, or were previously, employed."[1] A wide range of behaviors in the workplace classified as aggressive can contribute to the creation of a toxic and harmful work environment. Most of these behaviors are not the media-hyped coworker murders or assaults. Instead, they can include the following: dirty looks, obscene gestures, theft, sabotage, defacing property, hiding needed resources, showing up late for meetings, intentional work slowdowns, refusing to provide needed resources, yelling, delaying work to make others look bad, insults and sarcasm, spreading rumors, failing to transmit needed information, failing to warn people of a problem, failing to return phone calls, and giving people the silent treatment.

IDENTIFYING TYPES OF AGGRESSION: BUSS'S TYPOLOGY OF AGGRESSION

Aggression expert Arnold Buss developed a typology for classifying aggression. Buss proposed three dimensions for classifying aggressive acts: (1) physical/verbal, (2) active/passive, and (3) direct/indirect. The physical aspect refers to physical actions such as hitting or shoving the target, whereas the verbal aspect indicates using verbal communication to harm the target. The active aspect refers to how harm is inflicted by performing an action (e.g., insulting another), whereas the passive aspect indicates how harm is caused by withholding some action (e.g., failing to provide information, refusing to provide assistance). The direct aspect reflects how aggression may be aimed directly at the target (e.g., yelling at the target, refusing to answer a question from the target). The indirect aspect indicates how aggression may be expressed through an intermediary or by attacking something valued by the target (e.g., saying negative things about someone to coworkers, spreading rumors, or sabotaging equipment or files). These three dimensions can be used to create eight categories of aggression that have provided the foundation of much of the research on workplace aggression.[2]

Although the distinction between aggression and violence is an important one, it often is blurred in media reports of workplace violence. Violence typically is conceptualized to refer to intense cases of aggression, such as physically attacking one's supervisor and shooting a coworker. These actions are physical, active, and direct. In contrast, aggression typically refers to all behavior intended to do harm and includes a much wider range of behaviors than those that garner dramatic media coverage or are reported in national statistics on workplace violence. Because these less intense forms of aggression occur with more frequency, they typically are the focus of research. Moreover, these lesser forms of aggression can negatively affect the targets of the aggression, those who witness the aggression, and the organization itself.[3]

Studies employing the typology based on Buss's work usually investigate the more common, less intense forms of aggression, which seem to represent aggression that has "gone underground." The perpetrators may recognize that their intent to harm another will be perceived as deviant and inconsistent with the norms for appropriate workplace behavior. Hence, they channel their aggression into forms that are more difficult to detect and identify as purposefully harmful. They also may rely on aggressive strategies that seem prevalent and unpunished in their organizations. The perpetrators act strategically (and rationally) when they seek methods of inflicting damage that are not covered clearly in company policies. By going underground, their tactics protect themselves while accomplishing their objective of harming a target.

To investigate the nature and pervasiveness of workplace aggression, researchers often assess the frequencies with which employees have engaged in or witnessed these categories of behaviors in response to a variety of situations (e.g., negative performance feedback, workplace changes, perceptions of injustice, etc.). This research supports the idea that perpetrators go underground with their aggressive acts. These studies typically demonstrate that most aggression is less intense and falls into categories reflecting more covert, indirect, and passive forms of aggression.

Examples of this include the research conducted by workplace aggression experts Deanna Geddes and Robert Baron. Geddes and Baron's findings are consistent with the assumption that perpetrators prefer covert, indirect, passive forms over physical, active, and direct forms of aggression because the former types are harder to detect and punish. Covert forms of aggression (verbal, passive, indirect) often are more frequently reported than overt forms of aggression (physical, active, direct), presumably because hostile intent is more difficult to prove. For example, much workplace aggression includes behaviors such as talking behind someone's back and creating rumors about a target. However, some studies demonstrate that direct and indirect forms of aggression occur with about the same frequency or that direct forms occur more frequently.[4] Along these lines, Coombs and Holladay reported that people viewed verbal and passive forms as the most acceptable types of aggression. They found no differences in perceived acceptability between indirect and direct forms of aggression.[5] At first blush, the similarity in occurrence of direct and indirect acts seems contrary to the theory that perpetrators go underground. However, upon closer examination a reason for the lack of difference becomes apparent, as the effects for indirect and direct aggression can be explained by the effect/danger ratio.

CALCULATING THE CONSEQUENCES OF AGGRESSIVE ACTS: THE EFFECT/DANGER RATIO

The *effect/danger ratio* explains that covert rather than overt actions are more likely to be perceived as desirable. Covert actions are likely to be seen as "safer" because they would be less likely to incur punishment. Noted social psychologist Albert Bandura observed that direct attacks on others carry a high risk of retaliation. When attacks are difficult to interpret and it is not easy to assign blame or intent to the aggressor, aggressors are likely to pursue these tactics because they will be protected from counterattacks. The anticipation of punishment and/or retaliation reflects the danger component of the effect/danger ratio. The effect component indicates the anticipation of creating the desired result. Aggressors prefer behaviors that are effective in harming the targets while, simultaneously, incurring as little danger to themselves as possible. The effect/danger ratio reflects the subjective estimates of these two components.

Robert Baron and Joel Neuman speculate that verbal and passive behaviors are effective in maximizing the effect/danger ratio whereas indirect tactics may be less effective than direct tactics. This would lead perpetrators to prefer forms of direct aggression over indirect aggression. Although indirect methods are more likely to go unidentified, they may not bring about the desired result. This interpretation stemming from the effect/danger ratio would account for the similarities in frequencies reported in a few studies.[6]

In sum, motivated perpetrators will select aggressive acts that accomplish their goals while minimizing their chances of being caught and punished. The fear of punishment is tied to workplace policies against aggression. Perpetrators go underground in ways that circumvent those policies.

FACILITATORS AND INHIBITORS OF AGGRESSION IN THE WORKPLACE

What leads workers to respond with aggressive acts to organizational events such as negative performance feedback, employee monitoring, downsizing, and budget cuts? Researchers following Bandura's social learning theory note that situational cues in the workplace play a major role in influencing aggressive behaviors. They suggest it may be shortsighted to look at individual-level traits when searching for an explanation for aggressive behavior. They argue that aggressive behavior is learned by observing others engaging in aggressive acts (modeling) as well as through direct experience with aggressive acts (as the target and/or as the perpetrator). Reinforcers in the workplace can either encourage or discourage aggression. These reinforcers may take the form of (1) seeing others go unpunished for performing aggressive acts and/or personally not being caught or punished when engaging in aggressive actions (positive reinforcers) or (2) experiencing or seeing a coworker experience reprimands or punishments for aggression (negative reinforcers). Furthermore, if incentives in the organizational environment reward aggressive behavior (e.g., getting a promotion for being aggressive, receiving a choice assignment over another candidate because of belittling the opponent, pitting coworkers against one another in bidding for assignments, receiving a budget increase because you were the "squeakiest" and most obnoxious wheel), it is no wonder that employees engage in aggressive acts. A culture that tolerates and rewards aggression is likely to sustain aggression.

Individual traits (believing that aggression will lead to desired outcomes) as well as organizational characteristics (presence of aggressive models, aversive treatment, incentives for aggressive behavior) can contribute to a culture that views aggressive behavior as acceptable. Among the notable individual traits are Type A personality, low self-monitoring, and hostile attributional bias. The entry Contributors to Workplace Aggression provides details on these individual traits.

ASSESSING WORKPLACE AGGRESSION

The Workplace Aggression Tolerance Questionnaire (WATQ) is a 28-item instrument based on Buss's eight categories of aggressive behavior. Sherry Holladay and Timothy Coombs conducted studies to establish the reliability and validity of the instrument; the overall reliabilities (Cronbach's alpha) were .95 (study 1) and .97 (study 2). The instrument is unidimensional; items seem to be tapping into a similar aggression construct. In tests of convergent and discriminant validity, the WATQ demonstrated expected relationships with measures of verbal aggression and vengeance, and was not contaminated by a social desirability bias. The instrument also shows face validity, as it was derived by Buss's typology. Overall, the psychometric properties suggest that although Buss's eight categories of aggressive behavior are reflected in the 28 items, it makes sense to view the responses as an aggregate evaluation of the appropriateness of aggressive behavior.

When using the WATQ, researchers present respondents with a stimulus situation depicting a manager conducting a performance review with a subordinate. The subordinate believes the manager has been unfairly critical of his or her job performance and explains to the manager that the negative comments are inaccurate. However, the manager refuses to make any changes to the evaluation. The subordinate is aware that this negative review could prevent a pay raise and/or promotion. After reading the scenario, respondents evaluate the twenty-eight items describing actions the subordinate might take in response to the meeting. They rate the actions on a five-point scale ranging from "very inappropriate" to "very appropriate." Refer to the Guidance Appendix for a complete copy of the WATQ.

The performance review scenario was selected because previous research by Geddes demonstrated a link between (1) negative feedback situations and perceptions of injustice and (2) aggression. The scenario has strong ecological validity because its elements have been shown to be associated with aggressive actions toward the target (manager). The scenario also does not request the respondents to report on their own likely actions or to imagine they are the subordinates. Rather, the WATQ instrument asks them to report on the extent to which they would perceive a range of subordinate responses as appropriate.

Application of the WATQ

As noted above, most workplace aggression policies target overt, not covert, behaviors. The WATQ provides a reading of the tolerance people have for a wide array of aggressive behaviors. Tolerance for aggressive behaviors can be viewed as a risk, something that could develop into a larger problem. Forward-thinking companies try to identify and minimize risk. Companies conduct a number of different annual audits to assess various risks related to insurance and regulatory compliance. The risk of workplace aggression should be no different because it is as much organizational as it is individual. If an aggressive behavior is tolerated, people are more likely to engage it and to model that behavior for others. The risk becomes manifested into a problem. Using the WATQ can map tolerance in the organization and benchmark for training.

The organizational culture can serve to facilitate workplace aggression. Is aggressiveness mistakenly rewarded? An organizational culture can also be dysfunctional; however, we know that it is not monolithic but actually composed of a variety of subcultures. Consider a university. Cultural differences exist between faculty in different disciplines, maintenance staff, support staff, and health services personnel. By mapping subcultures with the WATQ, managers can determine whether certain areas of the organization are (1) more tolerant of aggressive behavior and (2) in need of additional training to address that risk. Though unidimensional, a very high score on a particular type of aggressive behavior suggests training should focus on that type of aggressive behavior. The WATQ can help to locate subculture-based risks and to inform workplace aggression training needs.

Organizations have been investing heavily in training efforts designed to reduce workplace aggression. The training ranges from awareness of the problem to strategies for defusing tense situations. At its base, training represents the need for people to realize a wide array of aggressive behaviors is problematic, should be deemed workplace aggression, and should not be tolerated in the workplace. The WATQ provides a means of determining whether the training is changing people's views of workplace aggression. Tolerance of workplace aggression can be benchmarked prior to awareness-oriented training. A few months after the training, the WATQ can be used to determine whether the training had any effect on tolerance of workplace aggression. Periodic checks could be made to determine whether the level of tolerance is decreasing, increasing, or remaining the same. Additional training can be used if the scores suggest an increase in tolerance.[7]

CONCLUSION

The dangers presented by workplace aggression extend far beyond workplace violence, its most visible form. In fact, managers find themselves dealing most often with the less visible forms of workplace aggression. Many types of workplace aggression that are given a foothold in the organizational culture can grow and transform from a risk to a problem. The WATQ helps to identify potential problem spots in the organization as well as problematic subcultures. Some areas of the organization may be more tolerant of workplace aggression and be in need of training. Yet training does not guarantee results. It must be assessed. It is crucial to know whether all forms of workplace aggression are deemed less tolerable because of training. Moreover, regular assessment with the WATQ provides evidence of longer-term success or failure of workplace aggression initiatives.

See also Contributors to Workplace Aggression; and Workplace Violence Prevention and Policies. See the Guidance Appendix for the Workplace Aggression Tolerance Questionnaire.

NOTES

1. Joel N. Neuman and Robert A. Baron, "Aggression in the Workplace," in *Antisocial Behavior in Organizations*, ed. Robert A. Giacalone and Jerald Greenberg (Thousand Oaks, CA: Sage, 1997), p. 38.

2. Neuman and Baron, "Aggression in the Workplace," pp. 39–41.

3. Neuman and Baron, "Aggression in the Workplace," pp. 39–41.

4. Deanna Geddes and Robert A. Baron, "Workplace Aggression as a Consequence of Negative Performance Feedback," *Management Communication Quarterly*, 10 (1997), 433–454.

5. W. Timothy Coombs and Sherry J. Holladay, "Understanding the Aggressive Workplace: Development of the Workplace Aggression Tolerance Questionnaire," *Communication Studies*, 55 (2004), 481–497.

6. Robert A. Baron and Joel N. Neuman, "Workplace Violence and Workplace Aggression: Evidence on Their Relative Frequency and Potential Causes," *Aggressive Behavior*, 22 (1996), 161–173.

7. Coombs and Holladay, "Understanding the Aggressive Workplace," pp. 481–497.

CONTRIBUTORS TO WORKPLACE AGGRESSION

W. Timothy Coombs

People in organizations often encounter adverse events or actions, which include financial pressures, increased stress, betrayal, lack of control, verbal threats, taking credit for other people's work, and criticism. These adverse events or actions can create anger, resentment, and frustration, which may result in workplace aggression. But an adverse event or action does not always result in aggression. Researchers studying workplace aggression have found two factors that help in determining when an unpleasant event or action will result in aggression: perceptions of justice and personal characteristics. Workplace aggression is a combination of conditions in the organization and personality traits. Understanding the factors that contribute to workplace aggression can help management develop mechanisms designed to reduce it.

PERCEPTIONS OF JUSTICE: ORGANIZATIONAL FACTORS

Adverse events or actions can be viewed as violations of justice. In organizations, the three variations of justice are distributive, procedural, and interactional justice. First, distributive justice involves perceptions of the fairness of outcomes. Employees determine whether the effort they put into their jobs results in equal rewards from their jobs. This evaluation is part of equity theory. Employees try to balance effort and reward in their jobs.

Second, procedural justice involves perceptions of the fairness of procedures. Are procedures implemented consistently, without bias; do they consider the interests of all parties; and do they provide a means for correcting errors? An example would be a performance appraisal. Are all employees evaluated using the same criteria? Is there a mechanism for employees to challenge inaccurate evaluations? Third, interactional justice involves perceptions of the quality of interpersonal treatment during procedural justice episodes. Did the people in charge of the procedural justice treat those involved with dignity and respect?

Violations of the three forms of justice can result in different forms of workplace aggression. If an adverse event violated only distributive justice, no workplace violence is likely. The perceptions of procedural and interactional justice should moderate the frustration and prevent workplace aggression. The employee is unhappy with the outcome but feels the process is fair and that he or she was treated well.

When the adverse event violates only procedural justice, an employee is likely to engage in verbal types of workplace aggression that target the organization. The employee is upset with the organization, so the aggression targets the organization. When the adverse event violates only interactional justice, an employee is likely to engage in verbal types of workplace aggression that target the offending person. The other person created the injustice, so the workplace aggression targets that individual.

When two or more forms of justice are violated, employees are more apt to move beyond words to workplace violence. The multiple violations intensify the frustration and anger created by the adverse event. The heightened "upset" can result in more serious workplace aggression, such as violence.

INDIVIDUAL TRAITS

Researchers noted that individual traits (believing that aggression will lead to desired outcomes) as well as organizational characteristics (presence of aggressive models, aversive treatment, incentives for aggressive behavior) can contribute to a culture in which aggressive behavior is viewed as acceptable. Among the notable individual traits are Type A personality, low self-monitoring, and hostile attributional bias. Type A people are frequently irritable and impatient and try to control the situation when they work with others. Type A personalities have been linked to aggression. Low self-monitors are not skilled at being socially sensitive and do not fit their words and actions to the situation. Researchers have found a link between low self-monitoring and obstructionism. Hostile attributional bias is when people perceive others as having hostile intentions even when such intentions are not present. These individuals are more likely to respond to events in an aggressive manner. These individual traits, which can be assessed, can contribute to workplace aggression.[1]

CONCLUSION

Employees will encounter adverse situations in the workplace that could trigger aggression. Whether or not they engage in workplace aggression is a function of their individual traits and organizational factors. A number of traits have been linked to aggression such as hostile attribution bias. However, these aggression-related traits are not proof a person will become aggressive. Employees who are screened and found to have these traits will benefit, as will all employees, from training on conflict resolution or other skills for decreasing aggression. The key organizational factors relate to perceptions of justice. Employees are less likely to be aggressive when they see the organization as just. Perceptions of justice include employees feeling that the procedures in the organization are fair and that managers are treating them fairly when applying the procedures. Actively working to maintain a sense of justice in the organization will help to reduce the likelihood of an adverse event resulting in workplace aggression.

See also Workplace Aggression; and Workplace Violence Prevention and Policies.

NOTE

1. Robert A. Baron and Joel N. Neuman, "Workplace Violence and Workplace Aggression: Evidence on Their Relative Frequency and Potential Causes," *Aggressive Behavior*, 22 (1996), 161—173; and Joel N. Neuman and Robert A. Baron, "Workplace Violence and Workplace Aggression: Evidence Concerning Specific Forms, Potential Causes, and Preferred Target," *Journal of Management*, 24 (1998), 391–419.

EMPLOYEE BACKGROUND SCREENING AND DRUG TESTING

W. Timothy Coombs

An employee background check or investigation is an inquiry into a person's character, personal characteristics, or general reputation. A number of different sources can be checked including criminal records, financial records, and driving records. A background check may even include a psychological evaluation, drug testing, or a physical. The type of background screening depends in part on the job qualifications. Driving records are critical if jobs include driving, whereas financial records are relevant to jobs involving finances. Employee background screening must protect consumer rights, comply with federal and state hiring standards, ensure a safe workplace, be part of homeland security, and avoid legal exposure.

Employee background screening is used for new hires and existing workers. Job applications can be checked for their backgrounds and drug tests. Current employees can be screened as well. Rescreening typically involves drug testing, random or follow-up, and periodic background rechecks. Background rechecks ensure that an employee's record has not changed. If there are changes that could place the company at risk, actions must be taken or else a negligent retention lawsuit could occur if an incident occurred involving that employee.

TYPES OF BACKGROUND SCREENING

Background screening can cover a wide array of information. The following is a list of thirteen common types of searches or screening activities.

1. *Social Security number trace.* This is done to verify the applicant's Social Security number. The trace determines whether the Social Security number belongs to someone who is dead and lists all the names and addresses associated with that Social Security number.
2. *Preemployment evaluation report credit report, or PEER*. A PEER uses the national credit bureau database to provide the applicant's national credit history. The report will reveal any bankruptcies, tax liens, foreclosures, or repossessions.
3. *County criminal record check*. This search, conducted through records of the clerk of county courts, is specific to that county only. This typically involves an on-site, manual search of records that cover the past seven years or longer as well as felony and misdemeanor filings.
4. *Criminal history search*. A criminal history search uses the Social Security number to construct a comprehensive criminal record search. A search is made of county records, as well as federal court records, for each address connected to the Social Security number.
5. *Statewide criminal record search*. Some states permit searches of their law enforcement or criminal records. The charges listed would include felonies, misdemeanors, and traffic violations.
6. *Federal criminal record search*. Searches can be conducted at any of the ninety-one federal district courthouses nationwide. The crimes covered in these searches would be violations of federal laws.
7. *Motor vehicle records check*. This search provides information on an applicant's driving history. The data would include speeding or moving violations,

chargeable accidents, DUIs/DWIs, suspensions or revocations, and accumulation of points.

8. *Employer reference check*. This search verifies past employment by checking with the human resource departments of previous employers. The search can check dates of employment and job titles. Applicants must grant approval for this contact.
9. *Education verification*. This search verifies all degrees claimed by the applicant. The information obtained includes the name of the institution, date of graduation, dates of attendance, degree obtained, and type or field of study. Applicants who are currently students can be checked for degree progress, field of study, and planned graduation date.
10. *Professional license verification*. This search verifies an applicant's professional license or certificate through the accrediting agency or professional association. This information includes the license number, expiration date, type of license or certificate issued, date of issue, and whether there have been any disciplinary actions or sanctions against the license or certificate holder.
11. *Military record verification*. This search contacts military branches to confirm dates served and type of discharge.
12. *Workers' compensation record search*. This is a search of an applicant's accident dates and nature or type of injuries involved. Such searches can be done only in states that permit the dissemination of workers' compensation claim history and must be used in compliance with the Americans with Disabilities Act guidelines. The State Workers' Compensation Commission of Industrial Relations Board will provide this data.
13. *Suspected terrorist watch list search*. This search determines whether the applicant is on a suspected terrorist watch list. See the Terrorist Watch List box.

BACKGROUND SCREENING AND LEGAL EXPOSURE

Background screening is a defense against negligent hiring and retention lawsuits. An employer can be held liable when an employee's actions harm someone. This can include attacks on coworkers or customers and some accidents. Employers have a duty to provide a safe workplace, and hiring and retention are a part of that. Employers should not hire or retain workers who pose a risk to others. This now includes intentional acts of violence. If an employee has a history of violence and attacks a coworker, the employer can be held responsible for the act. No employer is immune from negligent hiring lawsuits. However, a thorough background screening is a strong defense. The background screening should identify any red flags for the employer. If the applicant manages to hide the warning signs, the employer has shown good faith in trying to find the problems.

Negligent hiring occurs when a company fails to properly screen employees and the hiring results in injuries. Negligent retention takes place when a company keeps an employee on staff after learning the employee is an unsuitable worker and injuries occur. An employer must take corrective action such as retraining, reassignment, or firing when it discovers an employee is unfit for duty. There is also negligent supervision, which involves a failure to provide the proper oversight to ensure that employees perform their jobs properly. A taxicab company was held liable for hiring a driver with a history of criminal violence who later attacked a passenger. In another case, a security guard helped accomplices steal $200,000 in gold certificates. The security company was found liable for negligent hiring and supervision.[1] See the Minnesota Supreme Court's ruling in the Negligent Hiring box.

Suspected Terrorist Watch List

The following agencies or resources all can be contacted for suspected terrorist watch list searches:

- Office of Foreign Asset Control's SDN and Blocked Persons
- Federal Bureau of Investigation Alleged Suspects
- Suspected Terrorist List, National Counterterrorism Center
- Designated Foreign Terrorist Organization List U.S. Department of State
- Federal Bureau of Investigation's Most Wanted
- Office of the Superintendent of Financial Institutions—Individual Terrorism
- Office of the Superintendent of Financial Institutions—Entities of Concern to the Business Community
- Bank of England
- United Nations Sanctions List
- European Union List
- Sanctioned Countries Department of the U.S. Treasury
- Denied Persons List U.S. Department of Commerce Bureau of Industry and Security
- Unverified List U.S. Department of Commerce Bureau of Industry and Security
- List of Debarred Parties U.S. Department of State, Director of Defense Trade Controls
- Entity List U.S. Department of Commerce Bureau of Industry and Security
- World Bank Listing of Ineligible Firms

BACKGROUND CHECKS AND SECURITY

The concern over terrorism in the United States intensifies the need to verify employees. More importantly, background checks help to create a safer and more productive workplace. Screening may reduce theft and workplace violence, two important concerns for business security. Security is improved because the human risks are reduced through careful screening and evaluation of employees.

BACKGROUND SCREENING AND COST SAVINGS

In addition to avoiding the costs from liabilities for negligent hiring practices, background screening can help to lessen other operating costs as well. Background checks can reduce turnover by verifying that a person really is qualified for the job.

RESUME FRAUD

Resume fraud is rampant in the United States. The FBI estimates about half a million people in the United States make false claims about having a college

Negligent Hiring

The Minnesota Supreme Court has refined the central aspects of negligent hiring:

1. *Duty of care.* Employers must exercise reasonable care when hiring people whose jobs require that they have contact with the public. This contact places the public at risk for injury.
2. *Foreseeability.* The employer must anticipate how the employee's past could affect future actions. A bad driving record indicates an employee could have a vehicular accident. A history of violence demonstrates an employee could engage in a variety of violent acts in the future.
3. *Reasonable investigation.* Employers should investigate criminal backgrounds for jobs involving contact with the public. This is a reasonable precaution. Employers should also execute broader background investigation when the employee's application appears suspicious.
4. *Cause.* The hiring needs to determined to be the cause of the injuries. The employer placed others at risk by hiring the employee.

degree. The Society of Human Resource Managers believes that 53 percent of all applicant resumes have false information. Of the false information on resumes, 44 percent lie about work experience, 23 percent lie about credentials or licenses, and 41 percent lie about education. Applicants can buy diplomas from online "diploma mills" for under $500. These lies can create liabilities that cost companies money. The Association of Certified Fraud Examiners estimates that companies lose around $600 billion a year due to resume fraud.[2]

During interviews, behavioral interview techniques are an additional tool for checking work experience and skills. These techniques try to link the applicant's work experience to the current job. Based on the knowledge, skill, and abilities required for the job, interviewers ask applicants how they would handle a particular situation, such as "Describe an unpopular decision you had to make and how you implemented that decision." Or, "Tell me about a situation in which you influenced people positively through a presentation." Such questions provide insights into how applicants will perform, as well as expose job skills applicants might have embellished on their resumes.

Resume verification becomes an important step in the background check. The critical points on the resume to verify are education, work experience (especially job titles), previous employers (did the person really work there), specific job skills, and references (be wary of any glaring omissions in the reference list). Resumes should not be taken at face value.

DRUG SCREENING

Drug screening or testing is often a part of the background screening. Drug screening can help to prevent on-the-job accidents and reduce other business costs. Drug screening helps to lessen the costs of wages paid for absenteeism, wages paid for temporary staff to cover jobs, and costs of replacing damaged equipment; reduce sick leave; increase productivity; and reduce losses from theft. Around 80 percent of major U.S. companies conduct some form of drug testing. Drug tests can use urine, oral fluid, or hair as the samples. Drug testing minimizes negligent hiring by requiring all applicants to pass a drug test before being hired. Drug testing minimizes negligent retention by regularly testing employees and being prepared to intervene when a worker is identified as having a problem.

The legal situation for companies and drug testing involves two concerns. First, a company can be legally responsible if it does not drug test. If employees harm others while under the influence, the company can be held liable. Second, even well-intentioned drug testing polices can be challenged in court. Most of the challenges come in the form of right to privacy, freedom from unreasonable searches, and due process. Overall, the legal risk of not having a drug testing policy is greater than having one. A company can take actions to prevent successful legal challenges to a drug testing policy. A drug policy tells employees that they cannot be at work with "any detectable trace amount of drugs or alcohol in their system," not "under the influence" or "impaired." Drug tests identify the presence of drugs, not impairment from drugs. Drug testing should be kept confidential. Follow the testing standards set by the U.S. Department of Health and Human Services. See the Drug Testing Guidance box for information from the U.S. Drug Enforcement Administration (DEA).

WHY COMPANIES DO NOT USE BACKGROUND CHECKS

The two reasons for not using background checks are time and money. Some companies use so-called instant background checks. Though they are fast, they are not very accurate. It entails a computer search of a rather limited database. Thorough background checks are done by hand. The hand checks take longer and cost more money, but the client is getting more accurate and usable background checks. Poorly executed background checks are not a viable defense against negligent hiring lawsuits. Given the amount of money associated with the risks of hiring and retention, companies should be willing to pay for comprehensive background checks.

Drug Testing Guidance

Here are recommendations from the U.S. Drug Enforcement Administration (DEA) for steps to follow when implementing and maintaining a drug- and alcohol-free workplace program.

- Keep written records that objectively document suspect employee performance. These can be used as a basis for referral for testing.
- Know your employees. Become familiar with each one's skills, abilities, and normal performance and personality.
- Become familiar with common symptoms of drug use.
- Document job performance regularly, objectively, and consistently for all employees.
- Take action whenever job performance fails, regardless of whether drug or alcohol use is suspected.
- Know the exact steps to take when an employee has a problem and is ready to go for help.

Communicate immediately with your supervisor when you suspect a problem, and have a witness to your action when confronting an employee.[3]

Companies have a number of background screening companies to choose from. Keep in mind that background screening is becoming more professional. There's now even a professional organization, the National Association of Professional Background Screeners (NAPBS). The NAPBS, founded in 2003, has the following mission:

> The National Association of Professional Background Screeners exists to promote ethical business practices, promote compliance with the Fair Credit Reporting Act, and foster awareness of issues related to consumer protection and privacy rights within the background screening industry.
>
> The Association provides relevant programs and training aimed at empowering members to better serve clients and to maintain standards of excellence in the background screening industry.
>
> The Association is active in public affairs and provides a unified voice on behalf of members to local, state and national lawmakers about issues impacting the background screening industry.[4]

CONCLUSION

When hiring, always conduct a thorough background check that includes a criminal records search, employment verification, education verification, driving records, Social Security confirmation, suspected terrorist watch list check, and credit check. If you conduct the search yourself, be sure to follow all relevant laws, such as the Fair Credit Reporting Act. If possible, hire professionals to conduct the background check.

See also Security Guards/Officers; and Supply Chain Security.

NOTES

1. "A Look At Negligent Hiring Law Suits," online at http://www.verires.com/nhiring.htm (accessed 7 Feb 2007).

2. Mike Aamodt, "How Common Is Resume Fraud?" online at http:// www.runet.edu/~maamodt/Research%20-%20IO/2003-Feb-Resume%20fraud. pdf (accessed 7 March 2007).

3. U.S. Drug Enforcement Administration, *Guidelines for a Drug-Free Workplace*, 4th ed., Summer 2003, online at http://www.usdoj.gov/dea/demand/dfmanual/index.html (accessed 27 Jan. 2007).

4. National Association of Professional Background Screeners, "Background Screeening: Past, Present and Future," online at http://www.napbs.com/images/pdf/HistoryBackgroundScreening.pdf (accessed 15 March 2007).

VIDEO SURVEILLANCE

W. Timothy Coombs

Technology allows organizations to watch their employees, customers, visitors, and would-be intruders through video surveillance. Organizations can identify intruders, discover employee theft or other misbehavior, or prevent shoplifting. Video surveillance helps security to see what is going on in and around a facility.

EVOLUTION OF VIDEO SURVEILLANCE

Video surveillance is in a transition from analog to digital. Old video surveillance consists of the stand-alone CCTV systems that record to videotape, which are slowly fading away. Tape coding and storage is problematic, locating particular footage is time consuming, and tapes degrade over time and need replacing. Many companies are transitioning to the digital age with hybrid digital-analog systems. These systems connect cameras to digital video recorders, much like a DVR or TiVo.

Fully digital video surveillance is networked Internet protocol (IP) based. The video surveillance is a component of the IT network. Each camera has an IP address and is controlled centrally through a software application. The video surveillance transition to digital is another illustration of the convergence of physical security and IT security. (Refer to the Integrating Physical and Information Security entry for a further discussion of the topic.) The move to digital video surveillance is costly, requires additional training of security officers, and demands integration with IT.

BENEFITS OF DIGITAL IP SURVEILLANCE

The benefits of digital IP surveillance justify the costs. Digital IP surveillance provides superior visual data. The cameras have good lenses that can record in low light and even do thermal imaging. One digital camera can cover a larger area than an analog camera and zoom in for fine detail. The digital IP surveillance is integrated into the IT infrastructure. It can be on the regular server and enjoy the benefits of IT security and backup systems.

Digital IP surveillance is easy to centralize for monitoring and automation. Multiple facilities in geographically diverse locations can be connected to one monitoring center instead of having multiple monitoring centers at each site. The digital video is easier to archive and to retrieve or access. Retrieval takes a few mouse clicks rather than searching through racks of videotapes. Software helps to automate part of the video monitoring process and serves as an extra set of eyes to look for signs of trouble. An example is automated alarming that sends a warning signal when predefined signs are detected. The organization creates rules that help to identify a warning sign from normal activities. An example would be indications of human movement in an area where there should be no people or movement in an area during a specific time when there should be no people. These systems can differentiate between human and animal movements to prevent false alarms. The rules create a filter for detecting problems. Another example would be movement alerting a camera to switch to high-resolution mode and track the object.

Finally, digital IP surveillance has applications beyond security. Marketing departments can use the video to track the movement of customers through the store. They can determine how displays affect that traffic flow. The systems can also be used to work with safety systems and call for the fire department when needed.

Digital IP surveillance can be used for employee training and monitoring, sometimes called remote video auditing (RVA). RVA is much more than trying to prevent employee theft. Digital cameras are placed in locations to observe specific employee behaviors such as customer service or areas that involve regulatory compliance activities. The video is reviewed and critiqued by auditors, who can be consultants or in-house personnel. They then provide reports to management and employees at regular weekly or monthly intervals. RVA is currently being used in a variety of settings including health care, manufacturing, retail, food processing, and restaurants.

Feedback is an important component of goal setting and positive reward motivation systems. Both of these motivation systems have a high success rate across industries. However, neither works unless employees are given accurate feedback on their performance, which RVA does. Employees can see for themselves when they are acting properly or improperly. The video is used to show both good and bad examples to help employees learn how to improve their performance. RVA has assisted organizations in improving compliance scores, safety records, and customer satisfaction.

Plumrose USA is a meat-processing company. According to general manager Mike Rozzano, its facility was receiving poor performance safety reviews prior to using RVA. By employing an RVA system, Plumrose was able to identify areas that needed improvement and reward those areas with good performance. Safety review and employee morale improved with the RVA system. Employees could see their unsafe practices and examples of safe employee behavior. Clearly, digital IP surveillance has applications beyond safety and security.

PROBLEMS WITH VIDEO SURVEILLANCE

Some companies use fake cameras or hidden cameras as part of video surveillance. Security and legal experts agree that neither is a good idea. Fake cameras are designed to trick would-be troublemakers. However, safety manager Douglas Durden notes that fake cameras create a false sense of security for employees, customers, and visitors. Walter Palmer, a loss prevention specialist, adds that fake cameras can create a liability for negligent security when an organization has a responsibility to provide a certain level of security. In general, fake cameras do more harm than good.[1]

The same holds true for hidden cameras. Hidden cameras can violate surveillance policies and employees' right to privacy. Every company should have a clearly stated video surveillance policy that lets employees know where and how they will be observed. That policy should be well known and employees need to be regularly reminded of its reach. Lawsuits have reinforced the need for organizations to develop and publicize their video surveillance programs. Organizations do not have the right to use video surveillance just anywhere on their property; employees do have a right to privacy. Hidden cameras can create legal liability and angry employees. Before installing a surveillance system, then, you might want to consult with a local employment attorney to help draft a policy and set parameters for using the system.

CONCLUSION

Video surveillance has become much more than a person watching a television monitor and storing videotapes. Video surveillance is going digital and is becoming integrated with IT and IT security. The move to digital involves cost outlays in equipment. However, in most cases the many benefits of digital IP surveillance warrant the expense.

See also Crisis Sensing Mechanism; Integrating Physical and Information Security; Physical Security; and Supply Chain Security.

NOTE

1. Todd Datz, "The Hidden Camera," Sept. 2005, online at http:// www.csoonline.com/read/090105/hiddencamera_3824.html (accessed 20 March 2007).

COUNTERSURVEILLANCE

W. Timothy Coombs

Terrorism is a risk faced by most organizations. As the Terrorism entries note, terrorism can occur in the United States and in overseas facilities. Keep in mind that domestic terrorists in the United States include radical activist groups such as the Earth Liberation Front. (Refer to the entry Ecoterrorism for additional information on this topic.) Terrorist attacks are well-planned, not spur-of-the-moment, actions. Terrorists case a facility by visiting and collecting information many times before an attack. Organizations need to begin thinking like counterterrorism units. Security experts use countersurveillance to identify and prevent possible attacks. Among those advocating countersurveillance by organizations is Fred Burton, a former counterterrorism agent for the U.S. State Department. He is now a consultant and believes countersurveillance is the only means of identifying a potential terrorist attack.[1]

Countersurveillance is a process of collecting and analyzing data, something organizations regularly do. Countersurveillance seeks specific data on potential attacks. Security personnel begin by developing a list of potential suspicious activities, such as repeated visits by a person or vehicle. Suspicious activities narrow down the data to be collected and analyzed, the next step in countersurveillance. The final step is to take countermeasures.

Analysis is the most difficult part of the process. Companies, such as Abraxas Corporation, can provide software and training that facilitate the data analysis process. Abraxas has a software program known as TrapWire, which analyzes security information by looking for patterns of suspicious activities. Abraxas first examines an organization's physical vulnerabilities. The vulnerability analysis helps to determine what areas need to be monitored. It then installs TrapWire in the client's system. When security people see a suspicious vehicle or person, they open a TrapWire menu and enter information about it. The information can include physical appearance, types of vehicles, and license plate numbers. TrapWire then reviews the organization's security database (the security video) to construct a "PeoplePrint" or "VehiclePrint" profile for the suspicious activity. Based upon the security data, TrapWire creates a threat rating ranging from 1 to 100. The security personnel then take the necessary actions based on the threat level.

Other vendors that provide countersurveillance equipment and consulting help include Quest Consultants International, ADT, and Brink's Business Security.

Not every organization has the money to buy expensive computer-based countersurveillance systems. However, any organization can take a few simple steps to improve countersurveillance. First, train your employees to be observant. This means explaining that they should look for such things as unfamiliar people in an area, people without proper credentials, or unfamiliar vehicles parked nearby. Your people will be more effective if they know what they are looking for and why. Second, clarify whom employees should contact when they see something that causes concern. Employees should know whom to report specific suspicious behaviors to and the best way to contact those people. More than anything, countersurveillance is about people paying attention and reporting suspicious activities.

CONCLUSION

It is vital to remember that any countersurveillance is only as good as the people conducting it. Even advanced computer-based systems depend on security personnel noticing something suspicious and initiating the analysis. Relevant staff members must be trained in countersurveillance activities. This includes any staff that is in a position to spot suspicious activities. A vigilant staff is the key to effective countersurveillance. Successful countersurveillance, in turn, can save lives and protect organizational assets.

See also Agroterrorism; Corporate or Industrial Espionage; Crisis Sensing Mechanism; Ecoterrorism; and Terrorism.

NOTE

[1] Joseph Straw, "Countersurveillance Foils Attacks," *Security Management*, Feb. 2007, pp. 24–26.

RADIO FREQUENCY IDENTITY

W. Timothy Coombs

Radio frequency identity (RFID) may be the most controversial of any business security tool. RFID provides a means of tracking shipments through a supply chain, products in a store, and eventually paper money through the economy. This entry focuses on the security uses of RFID and concludes with some of the privacy issues that make it such a contentious security tool.

BASICS OF RFID

RFID is a system of technology components used to track "things." Its primary use is to follow the movement of items through the supply chain. As such it can be an important component in supply chain security. (Refer to the entry Supply Chain Security for more information on this topic.) The central component of the RFID is a wireless radio frequency device known as a tag. The tags are small devices that have a transponder and an antenna. They transmit data signals when powered/queried by an RFID on the tag's frequency.

RFID tags can have multiple frequencies depending upon their purpose, distance, and cost. Low-frequency tags cost a few cents and have a range limited to a few centimeters. High-frequency tags cost around fifty cents with a range of one meter. Ultra-high frequency tags are just over fifty cents with a range of seven meters. Microwave technologies cost much more and have a range of ten meters. The type of RFID tag an organization uses depends on the cost of the items being tracked and the nature of their transportation and storage. For instance, the transportation and storage may not permit close scanning so an ultra-high frequency or microwave tag may be required.

Unlike bar codes, RFID tags do not require a line of sight, do offer high-speed reads, and can make multiple reads. No power source is needed for passive RFID tags. Active RFID tags have batteries and attributes similar to wireless communication and sensing devices. Passive RFID tags are powered by the RFID readers or RFID printers. The reader sends an RF signal to the tag for power. The tag then transmits data to the reader. An RFID reader can write information to read/write tags in addition to collecting data. RFID printers can print information received from the tag and write some tags as well. RFID is governed by the electronic product code (EPC) standards. This ensures each tag has a specific and unique identity as well as providing a standard way to identify and exchange information between readers and tags.[1]

RFID PRIVACY CONCERNS

Privacy advocates are concerned that RFID could invade people's privacy. There is a web site devoted to the topic, http://www.stoprfid.com, and the charge is being lead by Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN). The concern is over the use of RFID tags on individual products, not on shipping containers. Each RFID tag has a unique signature. Retailers can use the RFID tag to link purchases directly to a person and track that individual's purchases over time. This is already done on a smaller scale through consumer loyalty cards. Retailers can create a more detailed picture of each consumer's buying habits. Retailers believe RFID tags provide an effective means of inventory control to identify out-of-stock items or excess inventory. Wal-Mart has been systematically adding RFID technology to its stores and requiring that its major suppliers implement the technology.

Clothing maker and retailer Benetton, for instance, had a plan to embed RFID tags in all of its retail items. The RFID tags would have allowed Benetton to track individuals and inventory their belongings by linking a buyer's name and credit card information with the serial number in an item of clothing. Benetton agreed to drop the plan after complaints from privacy groups.

Some privacy advocates see a much more serious breach of individual rights. The passive RFID tags remain active. When a customer enters a store, a retailer could read any item on or being carried by that customer that had an RFID tag and then use the RFID tags to track a customer's movement through the store. Some even fear an Orwellian world in which the range of detection improves and people can be located anytime and anywhere by RFID tags. Current technology does not allow such tracking, but privacy advocates fear it could be developed and limit people's ability to evade the technology.

Privacy advocates do provide advice on evading current RFID tags, how to search products for RFID tags, and how to disable RFID tags. They recommend puncturing or crushing the RFID tags, but not microwaving them. Microwaving will destroy an RFID tag but it can also cause the tag to catch fire.

CONCLUSION

RFID tags are an effective way to follow the movement of material and products through the supply chain (shipping) and to track inventory of individual products (retail). The RFID tags are low cost, are fairly easy to read, and allow readers to scan multiple items. RFID tags can be an important element in supply chain security. They let organizations know where a shipment is at all times, thus reducing loss through theft or misplaced items. They also let an organization know it is receiving the authentic items. The RFID tags have critics in privacy advocates. Their concerns are often overstated, but an organization must be ready to reply to criticism when it decides to utilize RFID technology as part of its security efforts.

See also Supply Chain Security.

NOTE

1. Craig Dighero, James Kellso, Debbie Merizon, Mary Murphy-Hoye, and Richard Tyo, "RFID: The Real and Integrated Story," 2005, online at http://developer.intel.com/ technology/itj/2005/volume09issue03/art09_rfid/p01_abstract.htm (accessed 5 March 2007).

BIOMETRICS

W. Timothy Coombs

A common question in security is "How do we know who someone is?" We need to know who people are to determine whether they should have access to physical locations (access to a building) and information assets (access to a computer system). Biometrics is one way of identifying who a person is as a prelude to access. Biometrics utilize body parts (physiological characteristics) and actions taken by a person (behavioral characteristics) to determine or verify identity. Biometrics can be used to permit entry to buildings, computers, e-mail accounts, Internet access, intranet access, and record the time of access and location of employees.

THE BASICS

Biometrics can use a variety of different physiological and behavioral characteristics to identify or verify a person. The physiological characteristics include fingerprints, iris recognition, retina recognition, facial recognition, and hand geometry. Behavioral characteristics include voice recognition, signature verification, and keystroke dynamics. A biometric system converts user information into a template. A user is then compared to that template for later matching. When a match occurs, the user is permitted access to the desired system or location.

A user "enrolls" by providing a biometric sample, which is assessed, processed, and stored. Later, a user provides a "submission," another sample, to be judged against the template. Biometric systems vary in reliability (number of false positives or negatives) and how acceptable the technology is to users.

We are most familiar with fingerprints. A simple reader is used to assess the fingerprint. Each fingerprint is unique. Many laptops now have fingerprint scanners built in. Fingerprinting is one of the most reliable and accepted technologies. Handprint geometry works in a similar fashion. Each handprint is fairly unique and can be read with a scanner. Currently, hand scanners cost a little more than fingerprint scanners. Facial, iris, and retina recognition are based on the unique features of these body parts. These scans are more invasive than fingerprint scans using cameras and other scanning technologies. Retina scans, for instance, require low-intensity infrared light, whereas facial and iris recognition require special cameras. These more invasive systems are resisted by users and are not as accurate as fingerprints. Retina scans are the most problematic because disease can change a person's retina.

The behavioral characteristics of biometrics are more susceptible to fraud than their physiological counterparts. Signature verification, sometimes called dynamic signature verification, examines a signature to see whether it matches the template using a signature tablet. You have probably used a signature tablet if you have ever charged an item in a store to a credit or debit card. Voice recognition examines voice samples. Keystroke dynamics, sometimes called typing rhythms, examines the way a person types on a keyboard. The ability to commit fraud with behavioral characteristics is not easy, but the risk for fraud is too high for many organizations that demand tight security.

CONCLUSION

Biometrics have a wide range of options and applications for business security. They are also a further illustration of the integration of physical security and information security. The identity of a person can now be verified by computers rather than individuals. The type of biometrics your organization uses depends upon the level of security that is needed, the amount of money you have to spend, and what types of biometrics your users are willing to accept.

See also Information Security; Integrating Physical and Information Security; Physical Security; and Portable Device Security.

SHELTER-IN-PLACE

W. Timothy Coombs

In an emergency, companies have two basic response options: evacuation or shelter-in-place. People are less familiar with the idea of shelter-in-place than evacuation. Shelter-in-place means that people should stay inside of buildings and seal the buildings off from outside air. For some reason, the outside air presents a danger. Shelter-in-place requests can be driven by chemical, biological, or radiological contamination in the air. At a company, shelter-in-place can affect employees, visitors, and customers. Anyone in the building must be notified of the situation, accounted for, and informed of what to do. Remember, you cannot force employees, visitors, or customers to shelter-in-place unless a government order has been issued. People have the right to leave if they choose to do so. An important part of preparation for your employees is to give them compelling reasons to stay inside.

HOW TO SHELTER-IN-PLACE

The basic steps to sheltering-in-place for a company include the following:

1. Close the business and post signs warning those outside the building.
2. Inform all those in the building, including visitors and customers, of the situation and the reason to shelter-in-place.
3. Shut and lock all windows and doors.
4. Have people assemble in designated rooms and bring disaster supplies to these locations. (Disaster supplies include nonperishable food, water, battery-powered radios, first aid supplies, batteries, flashlights, phones/phone access, garbage bags, duct tape, and plastic.) The National Institute for Occupational Safety and Health (NIOSH) recommends a variety of respirators that can be used during an evacuation to protect people from smoke inhalation. See http://www.cdc.gov/niosh/.
5. Have people call their emergency contacts to inform them of what is happening.
6. Turn off all heating, ventilation, and/or air conditioning. An employee who has been trained in the proper way to shut down these mechanical systems should do this.
7. Seal the windows and vents with sheets of plastic and duct tape. Ideally, the pieces of plastic are precut to fit the openings and employees are preassigned and trained in how to seal the windows and vents.

8. Seal around doors with plastic and duct tape.
9. Turn on the radio or television and listen for further instructions.
10. Once the all clear is given, remove plastic, restart the mechanical system, and go outside of the building until the old, possibly contaminated air in the system has been replaced with fresh, clean air.

From this list, we can identify three critical factors that must be considered before and during a shelter-in-place episode. First is the physical location of the shelter. The locations for shelters need be selected and designated, and people must be moved to those locations. Second is an accountability system. You'll need to take a head count, form a roster, post signs indicating shelter-in-place is in effect, and provide notification if a person leaves the shelter. Third is preassigning and training employees to shelter-in-place. Employees need to be assigned and know how to perform the task of sealing the building. It is essential to have a system in place so those sheltering can contact family members. The inability to contact family is the main reason people break with a shelter-in-place order. Security personnel can play a vital role during a shelter-in-place. Security personnel can help to ensure the facility is secure, provide direction to shelter areas, inspect the sealing-off efforts, and supervise the shelter areas.

When the need to shelter-in-place is a result of your company's actions, such as a chemical release, the responsibility for the shelter-in-place extends to the community around your facility. Community members need to understand that the warning signal means they must shelter-in-place, and they need to know what to do when they shelter-in-place in their homes. Companies work with area emergency personnel to inform residents about shelter-in-place and to warn them when such an action is needed. It is not uncommon in the United States for shelter-in-place warnings to be issued following an accident involving hazardous chemicals. According to Environmental Protection Agency statistics, there were 32 incidents requiring community members to shelter-in-place between 1989 and 1999.[2]

CONCLUSION

Some emergency situations or crises require people to shelter-in-place. Organizations must understand the equipment that is needed and the procedures to follow if there is a shelter-in-place order. As with other preparation efforts, organizations should conduct drills to test employee readiness for sheltering-in-place.

See also Benefits of Emergency Management; Disaster Recovery Management; Emergency Preparedness and Response Component; Exercise and Training Basics; Evacuation in Large and Multiple Tenant Buildings; and Emergency Response Training and Testing: Filling the Gap.

NOTES

[1] American Red Cross, “Shelter-in-Place in an Emergency,” online at http://www.redcross.org/services/prepare/0,1082,0_258_,00.html (accessed 5 May 2006).

[2] “Toxic Release Inventory Program,” online at http://www.epa.gov/tri/ (accessed 11 Feb. 2007).

EVACUATION IN LARGE AND MULTIPLE TENANT BUILDINGS

W. Timothy Coombs

One common security action all employees face is the evacuation of a building. It seems very simple—just leave the building. However, a successful evacuation requires careful planning and preparation. This entry reviews the key points for a successful evacuation, security's role in the process, and the challenges posed by multiple tenant buildings.

An evacuation is built around an emergency notification system and an active evacuation team. These two points constitute the evacuation plan. How do people know whether to evacuate a building? Again, this sounds deceptively simple. Recently, a university had trouble evacuating during an actual fire because people assumed it was a drill and kept working. People must know that when the warning to evacuate is given, everyone one must leave the building. Drills should be treated like actual emergencies. Management needs to convey the importance of always exiting a building when the alarms sound. Make sure emergency signage is visible, in working order, and in multiple languages if non-English-speaking people are ever in the building.

The evacuation team helps to ensure a safe and orderly egress from the building. Common evacuation team members include floor wardens, searchers, elevator monitors, stairway monitors, and ADA assistors. The floor warden, who runs the evacuation team, is in charge of a certain area during an evacuation. Searchers look in specified areas for people and mark areas as searched. This helps to make sure everyone is out of a particular area so that emergency personnel do not have to search those areas. Typical areas to search would include the copy room, offices, conference room, and bathrooms. Because people tend to congregate in these areas, they may not hear the evacuation notification.

Elevator monitors stand near the elevators to keep people from using them. Most elevators will automatically go to the ground floor and remain closed once an emergency notification is sounded. However, older systems or malfunctions could create a hazard. The elevator monitor prevents people from becoming victims of those hazards. Stair monitors in the stairwell tell people to go single file on the right side of the stairs. A single file on the right makes it easier for emergency responders to go up the stairs. During an emergency, people can forget and clog the stairs, so the stair monitor has an important job. Both monitors stay at their positions until the floor warden tells them to leave.

The ADA assistors are there to help anyone with disabilities to evacuate. An organization should talk with its employees ahead of time to find out who might need assistance and in what form. For instance, it may take two assistors to help an individual with a wheelchair. Organizations should consider purchasing special evacuation chairs to make the process even safer. It is a good idea to have extra assistors in case there are visitors needing extra assistance. The evacuation includes anyone who may be visiting your organization. These people require special guidance because they have not been a part of your drills. Everyone should be directed to the secure muster area.

Security is invaluable in an evacuation. It can help to identify who has left the building and is in the muster area. Some organizations use portable card readers to determine who is out of the building and in the muster area. Those records can be compared to security's records of who has logged in that day. Security is an excellent liaison with emergency responders. Security personnel can coordinate by supplying floor plans, locations of possible victims, evacuation status, and ADA employee locations. Security should secure the site as well, which includes establishing a perimeter and access points and providing access control to the site.

Frequently, organizations find themselves as one of many tenants in an office building. Multiple tenants add complexity to the emergency management process and can be illustrated with "simple" evacuations. Emergency management expert Patricia Bennett has found that the lack of integration between facility managers and the tenants' emergency managers/continuity managers is the main problem for evacuations of office buildings. The facility managers often do not communicate with tenants about evacuation and have little understanding of evacuations themselves. Bennett identified four common mistakes related to facility evacuations: (1) lack of communication about roles during an emergency (e.g., not knowing who will do what); (2) not knowing the real risks (e.g., failure to examine risks); (3) not knowing the audience (e.g., having signage in the right languages); and (4) not having a proper muster area (e.g., everyone trying to muster in the same location). These problems can be solved if residents and facility managers coordinate their evacuation plans and even have joint drills.[1]

Occupants of multiple tenant facilities should work together to develop and test evacuation plans. The same holds true for shelter-in-place plans. Evacuation and shelter-in-place are the two basic options in emergencies. Every organization should have its own emergency notification system and evacuation team in place before coordinating with others. Once the plans are developed, they must be tested in drills. Refer to the entry Exercise and Training Basics for the value of drills and the problems of failing to drill.

CONCLUSION

All organizations should create an evacuation team and train people for their various roles on that team. The organization should also hold regular evacuation exercises that involve everyone in the organization. For organizations in a multiple tenant building, be sure to coordinate your evacuation plans and exercise with the other tenants.

See also Exercise and Training Basics; Emergency Preparedness and Response Component; Shelter-in-Place; and Emergency Response Training and Testing: Filling the Gap.

NOTE

[1] Patricia L. Bennett, "Evacuation Planning: Four Mistakes Managers Make," *Disaster Resource Guide Quarterly*, Fall 2006, pp. 24–26.

INTEGRATING PHYSICAL AND INFORMATION SECURITY

W. Timothy Coombs

The heavy reliance on technology as part of the physical security system is the driving force behind the need to integrate physical security and information security. Technology on the physical side can track such activities as use of identification cards, biometric scans, facial recognition software, parking management, and the storage of closed circuit television (CCTV) video or digital video. Consider the CCTV system. The old analog version of tapes is being replaced with computer/web-based digital video. Add to this the computerization of fire systems and HVAC systems, two systems frequently linked to physical security, and we can see the trend.

Integration occurs on two levels. The first level is the integration of the various physical security systems. An organization needs to assimilate such physical security systems as parking, employee access control, CCTV, and visitor monitoring systems. The multiple physical security systems must work together and communicate with one another. Here are a few examples. An employee uses an identification card to move through various parts of the building. CCTV cameras are operating as well. Security officers can use a simple mouse click to create a report about that employee's access along with the accompanying video. A visitor signs in to meet with an employee. The visitor's driver's license is scanned into the computer and entered into the visitor system database including the license photograph. The employee is sent a text message that the visitor has arrived. The systems work in concert to make physical security more efficient and effective. For instance, if an employee's access requirements change, that can be added to the badge and access scanners. If an employee loses a badge, the reports from the access scans and input from the CCTV video can identify where the badge was used and capture the user on video.

The second level is to integrate the physical security system with other computer systems in the organization. This level includes integrating the physical security systems with the IT security systems. The IT security systems help to ensure the integrity of more modern, technologically advanced physical security systems. The second level also means using old-fashioned physical security to protect the IT hardware. One way to defeat IT security is to have direct access to the equipment. As security expert Salvatore D'Agostino notes, a combined system provides better protection from both physical and IT threats.[1] When an employee leaves an organization, the integration aids with security. The human resource system informs the security systems that the employee is no longer a part of the organization. The security systems immediately revoke that employee's access to physical and computer resources. The security systems can be used to monitor the employee's final exit from the facility.

INTEGRATION CHALLENGES

Integration sounds like a magical solution with all those different systems working in harmony. Historically, security systems have been proprietary and designed to be closed systems. They were difficult if not impossible to integrate with other systems. In others words, the security systems would not play well with others. More recently, security systems have improved integration by offering more open, standard systems and software kits to facilitate interfacing with other programs. Still, integration is not easy. The IT and security departments, like their system counterparts, will have to work together to make the integration work. Moreover, organizations may need to update the job descriptions and training for security officers. Security officers will need to be able to interact effectively with the technology that is part of today's advanced physical security systems.

CONCLUSION

Physical security is evolving, and that evolution is leading to the increased use of technology. To maximize the benefits of technologically enhanced physical security, an organization needs to integrate the systems with one another as well as other computer systems in the organization. Integration results in faster and more effective use of the physical security technology.

See also Information Security; Physical Security; and Video Surveillance.

NOTE

1. "Security Integration: Making It Work," March 2007, online at http://www.facilitiesnet.com/bom/article.asp?id=6273&keywords=security+integration (accessed 27 March 2007).

SECURITY ON A GLOBAL SCALE

Most people believe that technology continues to shrink the world. The size of the world has not changed, but it is easier for people to interact with others across vast geographic distances. Management may find its security and safety measures are complicated by its international connections. In particular, security on a global scale raises issues related to pandemics and supply chains.

PANDEMICS

Robert C. Chandler

A pandemic is a global disease outbreak. It occurs when a new contagion or communicable virus emerges for which there is little or no immunity in the human population, begins to cause serious illness, and then spreads easily person to person worldwide. Infected individuals experience the symptoms of the disease, including potentially serious ill effects, health consequences, or even death. Such a widespread illness strains the health care system and can create significant economic consequences for businesses, including disrupting travel, shipping, and transportation; impacting international commodities markets; high levels of employee absenteeism; lost productivity; disruptions in civic and infrastructure services; loss of key personnel and institutional knowledge; and a cascade of negative impacts spanning from vendors and suppliers to end-user customers and clients. It is impossible to predict precisely the time and severity of the next pandemic. Whenever and wherever a pandemic starts, everyone around the world is at risk. Countries might, through measures such as border closures and travel restrictions, delay the arrival of the virus but they cannot stop it. A pandemic is one of the most serious potential threats to business continuity, public health and safety, national security, and contemporary human civilization.

PANDEMIC PERIODS

The World Health Organization (WHO) and the U.S. Centers for Disease Control (CDC) and Prevention categorize pandemic status as having four distinct periods: (1) the interpandemic period, or between pandemics, (2) the pandemic alert period, (3) the (acute) pandemic period, and (4) the postpandemic period. Within each period various specific phases or stages are recognized as markers for pandemic alert. During the interpandemic period, a period of relative calm, there are no new or identified threatening viruses. In the case of influenza, for example, no new influenza viruses have been identified in animals, birds, pigs, other animals, and there are no new or threatening subtypes of a virus identified in humans. The interpandemic period can last for an indefinite amount of time, because it is really the pause between waves of pandemics.

During the pandemic alert period, the second major period, there is awareness of a pandemic threat and the potential for threats. There is not only an identifiable threatening virus detected in animals but also incidences of humans who succumb to the virus after having been infected by animals. In this period, small clusters of animal-to-human or perhaps even human-to-human transmissions, in very specific geographic areas, can be identified. There may even begin to be clusters of human-to-human transmission in a specific geographic region or epidemics on a local level.

During the acute pandemic period, the third major period, evidence exists of sustained human-to-human transmission in the general population in an expanding geographic area, and the virus jumps from one region to multiple regions and eventually becomes a global pandemic. The acute pandemic period is the time of active alerts and requires health control measures such as travel restrictions and quarantines. This would also be a period in which we might see waves of people succumbing in different demographic groups. The pandemic might affect the elderly first and then go through schools. Next there might be waves of secondary transmissions as the schoolchildren bring it home, and it thereby travels to different population centers. A pandemic period usually lasts anywhere from four to seven months, depending on the severity and the scale of the outbreak.

Also during the acute pandemic period, a substantial percentage of the world's population requires some form of medical care. Health care facilities can be overwhelmed, creating a shortage of hospital staff, beds, ventilators, and other supplies. The need for vaccine is expected to outstrip supply, and the supply of antiviral drugs is also likely to be inadequate early in a pandemic. Difficult decisions need to be made regarding who gets antiviral drugs and vaccines. There are significant infection rates with substantial consequences. The bottom-line number of fatalities varies depending on four factors: (1) the number of people who become infected, (2) the virulence of the virus, (3) the underlying characteristics and vulnerability of affected populations, and (4) the availability and effectiveness of preventive measures. The consequences of a pandemic transcend the numbers of sick, dying, and dead victims as businesses, schools, and many aspects of society are fundamentally disrupted during the acute phase of the pandemic.

Once the acute pandemic outbreak has subsided, we enter the fourth and last period, the postpandemic phase, which is a slow return to the interpandemic period with its preparations and threat monitoring for the next pandemic phase. The interpandemic period is the starting point of a new cycle. Potential pandemic viruses in animal populations during the interpandemic period may be seen, but have yet to be detected in humans. Because of the long history of pandemics, we recognize the basic cycle. This history also helps us take the appropriate preparedness measures and steps. Many organizational continuity planners may therefore want to tie the specific activation of their plans to the basic phases of a pandemic, and then communicate the period and actions required to the media as well.

PANDEMIC CONSEQUENCES

To begin to understand the scope of a potential pandemic impact, one need only look at the “routine” seasonal influenza outbreaks and project the impacts in geometric increments. The cold and flu season in a “normal” year is disruptive enough. It comes with tremendous loss in productivity, worker absenteeism, health costs, and lost opportunity cost. The seasonal flu itself is a health issue deserving some attention and preparedness in the event a sizable percentage of your workforce succumbs to it. For the public health sectors, the seasonal flu is a significant concern. However, the disruptions of the seasonal flu are only a minor sample of the disturbances that a fast-moving and widespread pandemic can unleash.

A pandemic brings with it substantial impacts and challenges. Each of its phases creates unique challenges, but the most significant impacts occur during the acute pandemic phase. The prime consequence to note is that pandemics happen quickly at the acute phase. A contagion can spread rapidly across the globe, and modern medicines and techniques can do little to stop it. For example, when an influenza virus emerges in even a remote part of the world, epidemiologists and world health authorities consider its global spread inevitable. The emergence of a new pandemic virus means that the entire world population could be susceptible. Individual countries might, through measures such as border closures, quarantines, and travel restrictions, delay its arrival or slow its spread, but such measures cannot stop a pandemic.

In the worst case, most people will have little or no immunity to a pandemic virus, and infection and illness rates will soar. A substantial percentage of the world's population will require some form of medical care. This suggests that the demand for health care access, at peak times, will be thousands of times greater than typical demand, which will stress and possibly overload health care systems. Death rates, moreover, are high, largely determined by four factors: the number of people who become infected, the virulence of the virus, the underlying characteristics and vulnerability of affected populations, and the effectiveness of preventive measures. Past pandemics have spread globally in two and sometimes three waves, creating an extended period of acute pandemic impacts thatlasts for a number of months rather than merely weeks.

The projections include forecasts that medical supplies and health care system capacity will be woefully inadequate during the peak periods of the next pandemic. The existing supplies of general antiviral drugs are likely to be insufficient during the initial phases of an acute pandemic period. There are efforts currently underway to develop vaccines that would be effective against many strains of the existing pandemic possibility, the H5N1 influenza virus (the bird flu). Some of these vaccines require multiple injections (spaced up to one month apart) in order to provide even limited protection. In clinical trials, such vaccines have prompted immune responses only strong enough to prevent infection in about 45 percent of study participants who received the full-strength vaccines.[1] Even these levels might help mitigate the impact of infection for those receiving the vaccines. However, they are not yet available commercially. (Typically, some vaccines are stored in the Strategic National Stockpile and used at the discretion of the national government for key high-risk individuals deemed essential to national security. The U.S. government's goal is to stockpile enough vaccine to protect up to 20 million people.)

Any existing vaccines will be slow to arrive (if at all) to the general public or specific enterprises and possibly will not be available until a second or third peak of the pandemic. Even when available, demand for such a vaccine is likely to outstrip supply, creating not only shortages but also problematic "lifeboat" decisions about who should receive vaccinations and on what criteria to base such decisions. A pandemic can create a shortage of health care providers (whose ranks will also be reduced due to infection and absenteeism), as well as of emergency department space, local health care provider slots, hospital beds, ventilators, and other medical supplies.

The pandemic will create economic and social disruptions. An especially severe influenza pandemic can lead to high levels of illness, death, social disruption, and economic loss. Everyday life will be upset because so many people in so many places become seriously ill at the same time. Impacts can range from school and business closings to the interruption of basic services such as public transportation and food delivery. Travel bans, closings of schools and businesses, and cancellations of events could have a major impact on communities and citizens. Significant worker absenteeism will be the result of those who are sick and dying, as well as those who care for sick family members or simply fear exposure by coming to the workplace. Some studies have forecast worst-case scenarios of over 50 percent absenteeism.[2]

Although a communicable virus might move rapidly across the globe, a pandemic disaster is a comparatively "slow-motion" disaster compared with tornadoes, hurricanes, industrial accidents, terrorism or criminal events, earthquakes, wildfires, or other types of catastrophic events. A pandemic may unfold in a series of peaks (e.g., waves), at which there are extremely high levels of infected and symptomatic people, each wave of which can last for six to eight weeks.

PANDEMIC RISK

Although many different possible contagions could spur the next pandemic, the most publicized threat source in recent years is the (cyclical) risk of an influenza virus. Influenza pandemics are recurring and unpredictable calamities that have occurred during at least the last four centuries and probably for longer than those recorded outbreaks. Since 1900, three major pandemics and several "pandemic threats" have arisen.

Influenza Pandemics

The Spanish influenza pandemic is the catastrophe against which all modern pandemics are measured. An estimated 20 percent to 40 percent of the worldwide population became ill and over 50 million people died. Between September 1918 and April 1919, approximately 675,000 deaths from the flu occurred in the United States alone. Many people died from this flu very quickly. Some who felt well in the morning became sick by noon and were dead by nightfall. Those who did not succumb to the disease within the first few days often died of complications from the flu (such as pneumonia) caused by bacteria. One of the most unusual aspects of the Spanish flu was its ability to kill young adults, and the reasons for this remain uncertain. With the Spanish flu, mortality rates were high among healthy adults as well as the usual high-risk groups. The attack rate and mortality were highest among adults 20 to 50 years old. The severity of that virus has not been seen since.

In February 1957, the Asian influenza was first identified in the Far East. Immunity to this strain was rare in people under 65 years of age, and a pandemic was predicted. In preparation, vaccine production began in late May 1957, and health officials increased surveillance for flu outbreaks. Unlike the virus that caused the 1918 pandemic, the 1957 pandemic virus was quickly identified due to advances in scientific technology. Vaccine was available in limited supply by August 1957. The virus came to the United States quietly, with a series of small outbreaks over the summer of 1957. When U.S. children went back to school in the fall, they spread the disease in classrooms and brought it home to their families. Infection rates were highest among schoolchildren, young adults, and pregnant women in October 1957. Most influenza- and pneumonia-related deaths occurred between September 1957 and March 1958, with the highest death rates among the elderly. By December 1957, the worst seemed to be over. However, during January and February 1958, another wave of illness broke out among the elderly—an example of the potential “second wave” of infections that can develop during a pandemic. The disease infects one group of people first, and infections appear to decrease and then they increase in a different part of the population. Although the Asian flu pandemic was not as devastating as the Spanish flu, about 70,000 people in the United States alone died out of approximately 2 million worldwide.

In early 1968, the Hong Kong influenza pandemic was first detected in Hong Kong. The first cases in the United States were discovered as early as September of that year, but illness did not become widespread in the United States until December. Deaths from this virus peaked in December 1968 and January 1969. Those over the age of 65 were most likely to die. The same virus returned in 1970 and 1972. The number of deaths between September 1968 and March 1969 for this pandemic was 33,800, making it the mildest pandemic in the twentieth century.

There could be several reasons why fewer people in the United States died due to this virus. First, the Hong Kong flu virus was similar in some ways to the Asian flu virus that had circulated between 1957 and 1968. Earlier infections by the Asian flu virus might have provided some immunity against the Hong Kong flu virus, which might have helped to reduce the severity of illness during the Hong Kong pandemic. Second, instead of peaking in September or October, as the influenzas had in the previous two pandemics, this pandemic did not gain momentum until near the school holidays in December. Because children were at home and did not infect one another at school, the rate of influenza illness among schoolchildren and their families declined. Third, improved medical care and antibiotics for secondary bacterial infections were available for those who became ill.

“Bird Flu”

Avian (bird) flu is caused by influenza A viruses, which occur naturally among birds. Wild birds worldwide carry avian influenza viruses in their intestines but usually do not get sick from them. Avian influenza is extremely contagious among birds and can make some domesticated birds, including chickens, ducks, and turkeys, very sick and then kill them. Infected birds shed influenza virus in their saliva, nasal secretions, and feces. Domesticated birds may become infected with avian influenza virus through direct contact with infected waterfowl or other poultry, or through contact with surfaces (such as dirt or cages) or materials (such as water or feed) that have been contaminated with the virus. This virus, which has not yet been detected in the United States, had infected about 300 people (with over 50 percent of the infections proving to be fatal) by early 2007.

In the mid- to late 1990s, another two avian influenza flu viruses—A/H9N2 and A/H5N1—were identified. Each of these caused illnesses among people after exposure to infected birds. Although neither of these viruses has yet gone on to start a pandemic, their continued presence in birds, their ability to infect humans, their very significant contagion and mortality rates, and the ability of influenza viruses to change and become more transmissible among people are ongoing concerns in the early part of the twenty-first century.

The risk from avian influenza is generally low to most people, because the viruses do not usually infect humans. H5N1 is the most deadly of the few avian influenza viruses to have crossed the species barrier to infect humans. The H5N1 virus has raised concerns about a potential human pandemic because of the following: it is especially virulent, can be spread by migratory birds, has already been transmitted from birds to other animals including humans, and (like other viruses) continues to evolve. A number of cases of human infection with A/H5N1 have periodically been reported in Asia in the past decade, and more than half of those infected with that virus have died. As of April 2007 there had been no sustained human-to-human transmission of the disease, but the concern is that H5N1 will evolve into a virus capable of human-to-human transmission at some point in the future.

Human influenza virus usually refers to those subtypes that spread widely among humans. There are only three known "A" subtypes of influenza viruses (H1N1, H1N2, and H3N2) currently circulating among humans with human-to-human contagion patterns. It is likely that some genetic parts of current human influenza A viruses originally came from birds. Influenza A viruses are constantly changing, and other strains might adapt over time to infect and spread among humans. Researchers are concerned that the continued spread of the highly pathogenic A/H5N1 virus across eastern Asia and other countries represents a significant potential threat to human health worldwide.

Most cases of H5N1 influenza infection in humans have resulted from contact with infected poultry (e.g., domesticated chicken, ducks, and turkeys) or surfaces contaminated with secretion/excretions from infected birds. So far, the spread of H5N1 virus from person to person has been limited and has not continued beyond one person. Nonetheless, because all influenza viruses have the ability to change, scientists are concerned that one day H5N1 virus could infect humans and spread easily from one person to another. Symptoms of avian influenza in humans have ranged from typical human influenza-like symptoms (e.g., fever, cough, sore throat, and muscle aches) to eye infections, pneumonia, severe respiratory diseases (such as acute respiratory distress), and other severe and life-threatening complications. The symptoms of avian influenza may depend on which virus caused the infection. Because these viruses do not commonly infect humans, the human population has little or no immune protection against them. If H5N1 virus were to gain the capacity to spread easily from person to person, a pandemic (worldwide outbreak of disease) could begin. No one can predict when a pandemic might occur. However, experts from around the world are watching the H5N1 situation very closely and are preparing for the possibility that the virus may begin to spread more easily and widely from person to person. No commercially available vaccine is currently available to protect humans against the H5N1 virus that is being seen in Asia, Europe, and Africa. A pandemic vaccine cannot be produced until a new pandemic influenza virus emerges and is identified; there is always some delay in developing vaccines from the emergence of a new contagion virus.

CONSEQUENCES OF THE NEXT INFLUENZA PANDEMIC

In the twentieth century, three influenza pandemics caused high death rates and great social disruption. Although health care has improved since the last one, epidemiological models from the Centers for Disease Control and Prevention project that a pandemic is likely to result in from 2 million up to 7.4 million deaths globally. Losses to businesses are projected to range upward to over $100 billion worldwide for a moderate to severe pandemic due to transportation limitations, disruptions to the commodities markets, productivity losses due to absenteeism, business continuity disruptions, personnel losses, and unusual medical and health care costs.

According to the WHO and CDC, if an influenza pandemic were to appear, the following could be expected:

- Given the high level of global traffic, the pandemic virus may spread rapidly, leaving little or no time to prepare.
- Vaccines, antiviral agents, and antibiotics to treat secondary infections will be in short supply and unequally distributed. It will take several months before any vaccines become available.
- Medical facilities will be overwhelmed.
- Widespread illness may result in sudden and potentially significant shortages of personnel to provide essential community services.
- The effect of influenza on individual communities will be relatively prolonged when compared to other natural disasters, as it is expected that outbreaks will reoccur in a series of peaks or waves.

PREPARING FOR THE NEXT PANDEMIC

Central to preparedness planning is an estimate of the deadliness of the next pandemic. Experts' answers to this fundamental question have ranged from 2 million to over 50 million. The disruptions to society, families, businesses, and the national economy may be substantial. Although pandemic preparedness planning has dramatically increased, a large number of businesses and organizations are still underprepared for the threat of a pandemic.

Pandemic preparedness includes the necessity to allocate resources (money, time, personnel, and efforts) for creating a pandemic plan and a pandemic communication plan. Look beyond the boundaries of your business, and consider whether your suppliers, contractors, vendors, and distributing channels are also prepared for pandemic risks. The threat of a pandemic should be monitored.

It is also vital that your plans establish policies to adjust to and accommodate for the disruptions that a pandemic will create. Consider revising sick leave policies, benefits (bereavement and health care), hygiene and social distancing protocols, cleaning procedures, alternative work (off-site or telework), travel policies, and contingency (backup) plans for all aspects of your business operations. It may also be necessary to stock emergency supplies such as masks, gloves, and supplies for those who may be isolated at home or work, or even medical stockpiles (possibly including antiviral medications). Prepare your people to minimize their risk of becoming infected, and know how to cover for the anticipated personnel shortages. Explain pandemic sick leave policies or alternative work arrangements. Have a specific response plan in place for the first warnings of a pandemic outbreak. One of the most critical aspects of surviving a pandemic is to have a comprehensive pandemic communication plan.

Steps Toward Pandemic Preparedness

The following are key steps generally acknowledged as essential for moving toward pandemic preparedness.

1. Secure a senior management commitment to pandemic preparedness.
2. Identify a pandemic preparedness coordinator.
3. Conduct a pandemic business impact analysis (BIA).
4. Establish pandemic HR policies.
5. Create a pandemic communication plan.
6. Create a pandemic response plan (including activation criteria).
7. Establish a threat monitoring system.
8. Work with insurers, vendors, and customers to ensure a coordinated response.
9. Train and prepare your workforce, customers, and constituents for pandemics.
10. Test, practice, and revise your pandemic plan.

CONCLUSION

It is impossible to predict exactly when the next global pandemic will strike. However, the scientific consensus makes one point absolutely clear: pandemics are recurring events and another pandemic will occur. Disaster management and recovery plans have long sought to ensure business continuity by seeking to protect and have alternatives to losses of information technology, data, buildings, and equipment. The new reality is that no disaster management or recovery plan can be considered comprehensive or complete if it does not address the inevitable next public health disaster—a global pandemic.

See also Business Continuity; Crisis Communication: External and Internal; Crisis Management, and Pandemic Communication.

NOTES

1. Lisa Schirring and Robert Roos, "FDA Approves First H5N1 Vaccine," 17 April 2007, online at http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/apr1707 vaccine.html (accessed 20 April 2007).

2. "Pandemic Planning Assumptions," 13 Sept. 2006, online at http://www.pandemicflu .gov/plan/pandplan.html (accessed 20 April 2007).

PANDEMIC COMMUNICATION

Robert C. Chandler

A pandemic is a global disease outbreak. It will strain the health care system and can create significant economic consequences for businesses including disrupting travel, shipping, and transportation; impacting international commodities markets; high levels of employee absenteeism; lost productivity; disruptions in civic and infrastructure services; loss of key personnel and institutional knowledge; and a cascade of negative impacts spanning from vendors and suppliers to end-user customers and clients. It is impossible to predict precisely the time and severity of the next pandemic. The threat of a pandemic is one of the most serious potential threats to business continuity, public health and safety, national security, and contemporary human civilization.

According to the World Health Organization (WHO) and the U.S. Centers for Disease Control (CDC), even in the best-case scenarios of the next pandemic, 2 million to 7 million people would die and tens of millions would require medical attention. If the next pandemic virus were a very virulent strain, deaths could be dramatically higher. The global spread of a pandemic cannot be stopped but preparedness can reduce its impact. It is of central importance that businesses take the necessary steps to develop their own preparedness plans. Some have already implemented structures and processes to counter this threat; however, the plans of others are far from complete and many organizations have yet to begin.

WHO believes the appearance of H5N1, now widely entrenched in Asia, signals that the world has moved closer to the next pandemic. Although it is impossible to forecast the magnitude of the next pandemic accurately, it is clear that much of the world and many businesses and organizations are unprepared for a pandemic of any size.

A pandemic will significantly disrupt your business operations. Consider the following: key personnel may be unavailable for substantial periods of time or may be lost permanently; organizations will need to communicate to and notify different key target audiences representing various demographics; the crisis will create pressures, constraints, and stress, which in turn will negatively affect access, comprehension, and compliance with messages; misunderstandings and rumors will create havoc; key people will hunger for accurate and useful information; and updated two-way communication will be of the utmost importance to the functionality of your operations and care for your people. Every organization needs a pandemic communication plan to mitigate, survive, and recover from a pandemic disaster.

Some projections estimate that, at peak periods, approximately 40 percent (or more) of the workforce may be absent from their duties during a pandemic. Operational, as well as personal, financial, and safety, messages critical to your operations will need to be disseminated and confirmed. These communication challenges will occur when people are too distracted, preoccupied, and overstressed with the pressures of the crisis to devote all of their attention to trying to understand and comply with such messages. This creates a very difficult communication problem. Prudent companies should thoroughly prepare and have various communication contingency plans in place to sustain coordination and communication with all key constituents before, during, and after a pandemic crisis. The pandemic communication planning process is a key priority for overall pandemic preparedness, because in the end, your pandemic communication plan must be prepared to overcome these challenges.

PANDEMIC COMMUNICATION PLANNING

All businesses face common communication challenges during crises, including receiving inaccurate, incomplete, and contradictory information, especially early in the critical events; rapidly changing circumstances; and a variety of sensitive HR and personnel information issues. By their very nature, crises are usually beyond the power of “routine” processes and procedures. The methods, processes, procedures, and even people that handle the day-to-day events cannot be consistently relied upon to successfully manage crisis events and ensure the survival of both your people and your business. You must anticipate the particular communication needs for your organization during a pandemic outbreak. Be prepared to take the initiative to communicate effectively despite the disruptions and people out of their usual position. Assume that there will be breakdowns of “routine” systems and technologies during the peak periods of a pandemic. Your target audiences (both individuals and teams) will experience high levels of stress, and all these factors present an additional level of communication challenges to prepare for. Although pandemics are “slow-moving” disasters compared with many other types of threats, rapidly occurring events/changing information on a local level will challenge your communication plans. People will aggressively demand information during a pandemic. All of the decisions about when to communicate, how, and to whom will be subject to the critical analysis of your stakeholders, your constituents, the news media, and the general public.

Prepandemic education and outreach are critical to both preparing your audience for the pandemic as well as prepositioning knowledge with your audiences that will aid your messages' effectiveness during an outbreak. Understanding what a pandemic is, what needs to be done at all levels to prepare for pandemic influenza, and what could happen during a pandemic helps in making informed decisions both as individuals and as a nation. During the pandemic, the public must be able to depend on its government to provide scientifically sound public health information quickly, openly, and dependably. The capacity to assess risk and employ effective mechanisms to mitigate and manage risk has advanced far, but one key factor to the success of any risk management is risk communication.

Pandemic communication planning begins with self-assessment. First you need to determine the basic objectives of your communication plan. Determine to whom and with whom you need to communicate before, during, and after the pandemic. Clarify how you intend to reach these key audiences, what your alternative channels (modalities) are for connecting with them, when and how often you will need to communicate, and whether the capability exists for two-way/interactive communication. Then create specific messages to have available for use (to provide information, warnings, notification, and requests for behavioral compliance). Finally, test, revise, and continue enhancing your communication plans to be ready when the pandemic unfolds.

A pandemic communication plan should detail how your organization plans to communicate (and who is responsible for each action) with the following potential target audiences during and following a disaster: employees/families, customers, suppliers/vendors/partners, local community, emergency responders, government authorities, and the news media.

RISK COMMUNICATION

Risk communication, as described by the U.S. Department of Health and Human Services, is an interactive process of exchanging information and opinion among individuals, groups, and institutions. It often involves multiple messages about the nature of risk or expresses concerns, opinions, or reactions to risk messages or to legal and institutional arrangements for risk management. Any written, verbal, or visual risk message contains information about risk that may or may not include advice about risk reduction behavior. A formal risk message is a structured written, verbal, or visual package developed with the express purpose of presenting information about risk.

Effective risk communication requires a proactive plan. Merely disseminating information without regard for communicating the complexities and uncertainties of risk does not necessarily ensure effective risk communication. Systematic, thorough, and validated testing efforts will help guarantee that your messages are constructively formulated, transmitted, and received, and that they result in meaningful actions. Successful risk communication messages can assist in preventing ineffective, fear-driven, and potentially damaging responses to pandemic crises. Appropriate risk communication messages can create trust and credibility, which are vital in a pandemic.

Here are some general guidelines for effective risk communication, which can prevent making the crisis worse with inadequate messages or failure to communicate effectively:

- Have clear goals and objectives for your communication plan.
- Develop "message maps" in advance for all key audiences and phases of the pandemic. (There's more to come on message maps.)
- Give your target audience specific behavioral guidance on what to do/how to respond.
- Test your communication plan and messages—assess and evaluate. During the pandemic, consistently stay on message.
- Plan your communication to ensure timely and accurate information. Your messages should disclose real risks and be honest, frank, and transparent. When in doubt, acknowledge uncertainty. Your risk communication should create and sustain your credibility.
- Avoid unnecessary communication of complex, medical, technical, or scientific information.

Accurate, timely, and appropriate information reassure your audiences.

INFORMATION DISSEMINATION

As a general rule, more information (rather than less) is usually better during crises. However, the nature of communication during pandemics must consider specific and more complicated questions of timing, load, and source credibility, which make the decisions about how much information to include difficult. Sometimes, too much information is just as problematic as too little information. Getting the appropriate amount of information to the right people at the right time is vital. Underloaded messages serve no purpose at all. Overloaded messages, containing too many details and too much information, tend to overwhelm the receiver, and important parts of the message are "lost."

Determining how best to get the word out is another aspect of pandemic communication planning. You must decide what information is crucial to convey in messages during a pandemic in order to secure comprehension, understanding, and also prompt appropriate audience responses. Likewise, it is important to decide what messages should be delivered prior to, during, and after a pandemic and via which channels or modalities. Also, you must anticipate the possible breakdowns and obstacles to effective communication and how to minimize these weak points. Although every organization is unique, consider the following factors in your information dissemination and emergency notification communication planning: evacuation or shelter instructions; notification or activation of emergency operational procedures; warnings; rumor control information; resumption-of-operations information; assembly-of-security information; emergency operations center (EOC) functions as well as "command, control, and coordination" (C3) messages; response to phone line jams and loss of Internet services; response to media intrusion, inaccurate reports, and mistakes; and how to stay in touch with your people as they are out of place or scattered during the pandemic.

Information must arrive to the appropriate recipient at the optimal time via the best channel—misrouted, tardy, or misdirected information delivery is a significant problem during a crisis such as a pandemic. Those who receive the information must also be able to recognize and understand it. Review your communication technology and anticipate the impact of breakdowns in communication systems. What are your backup modalities if phone lines are down or Internet servers are off-line? What vulnerabilities exist due to outmoded or inadequate notification technology (e.g., is your company still using a traditional "manual calling tree" system for emergency notification)? Is your contact information database outdated or unreliable? Do you have the capacity for multiple channels of notification or automated notification? Is there multiple two-way communication capability?

MESSAGE CHARACTERISTICS

Much could be written about the quality of pandemic communication messages. Obviously, emergency warning or notification messages should be precise, transparent, oriented toward actions, compassionate, and framed in personal terms relevant to the audience. The risk communication messages you create before, during, and after a pandemic should be prioritized (state the most important facts at the beginning of the message) and factual (do not downplay risks or exaggerate facts). Avoid any unnecessary speculation. Remember that word choice is critically important both for the messages and their implications as well as for the "tone" of the message.

META-MESSAGES AND FRAMING

Meta-messages are literally messages about messages. More generally, these are (usually implicit) interpretative clues that provide the audience with cues to guide their understanding of messages. Meta-messages are the deductions that one gains by "reading between the lines" in an interpretive process to discern the tone, urgency, or implicit (but unstated) meanings of a message. Some meta-messages are deliberate (e.g., staging, context, putting points first or last in a message, etc.). Others may not be intentional, but nonetheless audiences "decode" them believing that they have "understood" or "gotten the message," even though such understanding originates from their own perceptions and interpretations rather than any deliberate construction of the message.

Perhaps the most basic meta-message can be illustrated with the language function of irony. Irony is revealed by context and/or nonverbal behavior that alerts the audience that the message is something other than/more than what the words themselves mean. Irony can transform a salutation of "good morning" into a belligerent confrontational challenge. Meta-messages are more generally the messages between the lines that guide audiences' interpretation of what they are hearing or reading. Meta-messages usually exist as either intentionally positive or unintentionally negative. Meta-messages may include the setting (location, context, etc.), nonverbal communication behaviors (tone, timing, appearance, movement, etc.), presence/absence of specific individuals, topics/issues discussed (or not discussed), or any other aspect that can be taken as a hint of something more than what is literally being said.

Obviously negative meta-messages can undermine your message strategy and perhaps even have the reverse persuasive effect on your audience than what you intended. Thus, on one hand, it is essential to exercise caution about potential negative meta-messages that can undermine your communication goals. Critically evaluate how your audience could (mis)understand and (mis)interpret elements of the message or the medium. On the other hand, consider the strategic use of meta-messages to bolster the effectiveness of your communication. Think about how you can embed meta-messages that are consistent with your message, and be attentive to the setting and timing of your communication.

Framing refers to the process by which selective words, narratives, or terminology subtly influences how audiences interpret or evaluate otherwise objective information. Framing includes labels and embedded words as well as how information is packaged. In political contexts this is related to the idea of "spin" and "spin control." Words function as form of label that defines the reality for the audience. The classic illustration is the maxim that one side's *freedom fighter* is the other side's *terrorist*. In this case, specific word choice determines the persuasive interpretation of all other elements presented and carries with it the "implications" of guilt embedded in concepts associated with one word or the other.

Framing also sets the parameters of defining the issue for the audience. A common illustration of this principle is in the social controversy over abortion rights. It is significant that each side of this debate self-describes its position with a one-sided polarized term, which in turn implicitly (negatively) defines its opposition. Therefore, the "pro-life" position is juxtaposed by implication with the "anti-life" position, as is the "pro-choice" side with the "anti-choice" position.

Let's examine one dramatic example to demonstrate the concept of framing in the context of communicating in the midst of a pandemic. One could use different words (labels) to describe those infected with a virus, calling them *infected*, *victims*, *patients*, *ill*, *contagious*, *sick*, *sufferers*, *carriers*, *symptomatic*, or in the end *survivors*. Perhaps some of these are extreme examples, but I use them to illustrate the point. Each term carries with it a set of implications that implicitly frames the nature of the act under question. The reality is that many, if not all, of these terms are correct at some level for describing the act/person/situation in question. Nonetheless, when thinking about these word choices in the relative calm of the prepandemic period, referring to someone as *infected* or a *carrier* of the virus brings with it a number of depersonalizing implications and spins our perception of that person in a dehumanizing (and threatening) direction. It is even possible that such word choices could help sustain the "logic" of mistreating or discriminating against someone during a pandemic.

Some of these words unnecessarily play on our fears and prejudices. Other words instead call upon the spirit of our "better angels" and point us in a more positive direction. It is imperative, however, to recognize and understand the framing implications of these word choices. In the past pandemics, hysteria and fear were fueled by some of the language used, the meta-message (between the lines) implications of those words, and the way that the crises were framed. Careful consideration of communicated frames and the role that they play to facilitate the interpretative process and guide the audience toward particular conclusions is very important.

In its most basic manifestation, framing can influence the agenda of the expected communication topics and information. In its strongest expression, framing can serve as a subtle aspect of persuasion capable of changing opinion, shifting attitudes, and motivating specific action among the audience.

RUMORS, MISINFORMATION, AND ERRORS

Rumors will happen during a pandemic. Rumors have always thrived during public health emergencies and tend to emerge in almost every category of disaster or crisis. This is due, in part, to the state of heightened emotional responses, the inherently limited availability of accurate and timely information, and the tendencies for narrative weaving during these events. This combination of elements gives rise to rumors, gossip, speculation, assumptions, inferences, and no small number of conspiracy theories. Obviously, in this modern age of instantaneous communication, the Internet, and personal weblogs (blogs), the unstable local information environment extends electronically. It is important that your pandemic crisis communication plan include specific strategies to respond to substantive rumors, speculation, and misinformation as they circulate.

When responding to a rumor or widespread misinformation, consider how the rumor was initially generated and how it might further evolve as well as spread to new audiences. This may be helpful in designing a communication response that "nips the problem in the bud." As you plan, note that it is important to move quickly to correct these examples of dysfunctional communication; that you will need to keep the level of your response appropriate to the level of the problem; that overreacting to an isolated statement of error might attract attention to the very inaccurate "fact" you are trying to correct; and that underreacting to widely reported erroneous information might allow for a compounding of the error. If a significant rumor is confined to a small audience, then focus your corrective communication to those connected with that group. On the other hand, if misinformation or a rumor is widely known and spreading, you may need to communicate to the broadest possible audience or even consider mass media options.

MESSAGE MAPS

Message mapping is an important process for developing clear and concise message templates that will expedite your communication during a crisis. Message maps are navigational charts or road maps for plotting the risk communication messages that you will need to utilize during and after a critical event. Message maps, developed in advance of a crisis, are detailed, systematically organized, "prepositioned" responses to anticipated message needs, informational issues, questions, or concerns in your various target audiences. Message maps should be constructed according to the principles of effective communication, audience perception and information processing tendencies, and the goals and objectives for your pandemic crisis management. Message mapping and the generation of specific message map templates are crucial to ensuring that an organization has a central repository of effective, consistent, and easy-to-use messages at each stage of the pandemic.

Message maps can be very useful in helping an organization reach its communication goals before, during, and after a pandemic. Message maps should be created well in advance of the pandemic outbreak, linked to different periods/phases of the pandemic, and adjusted for maximum effectiveness with specific target audiences. Every organization needs to have a set of message maps for its particular situation. Message maps should contain adjustments for different demographic groups—including language, education, life situation, and occupation or work role—and cover all of the information agenda questions of most importance to each category. The process of mapping messages for pandemic communication takes time and energy. It should involve a number of different perspectives across the organization.

As you develop maps, consider people affected, walk through every possible outbreak scenario for each period and phase, make choices about types of messages, determine channels of communication, and hone and refine actual message maps. It is also useful to test messages to have a sense of how various audiences will perceive, interpret, understand, comprehend, and respond to these messages.

Message maps can help you connect with your key audiences. Achieving and sustaining effective communication with your target audiences depends (in part) on selecting channels (modalities) of communication that reach them and allow them to reach back to you. Consider both your messages and your target audiences in selecting the most appropriate communication notification systems.

THE ROLE OF AUTOMATED MASS NOTIFICATION IN PANDEMIC COMMUNICATION

Automated mass notification systems can help address common pandemic challenges. These tools enable communicating quickly, easily, and efficiently with large numbers of people or targeted groups of people in minutes, not hours. They allow you to utilize all contact paths, including the preference list of communication devices provided by the targeted audience. These capabilities are especially important when regional or local communication infrastructure is damaged or not working. These emergency notification systems can help ensure two-way communication before, during, and after the pandemic as well as reduce miscommunications and squelch rumors with accurate, consistent messages. By automating manual, time-intensive, error-prone processes of initiating communication during the pandemic, automated systems can free up key personnel at the periods of high absenteeism so they can perform other critical tasks. These systems can improve communication effectiveness by eliminating any single point of failure. And they can be designed and maintained “in-house” or outsourced to an external provider. Typically these systems are easier to use and require only a modest investment given their capacity to enhance your communication during a pandemic crisis. There are many different vendors and providers for the automated notification technology and services; however, one of these companies—3n (National Notification Network)—also provides a pandemic communication message/content solution foundational product, which I have developed, that you might consider to aid your own planning. You can find more information about 3n in the Resource Appendix under Vendors.

CONCLUSION: PANDEMIC COMMUNICATION READINESS

Your pandemic communication planning goals should ensure that you can fulfill all of your critical communication goals and objectives before, during, and after a pandemic outbreak. You should be able to demonstrate the capability of reaching your target audiences (key people with whom you need to communicate) with valid messages in a reliable, confirmable, and efficient way.

When testing and validating your pandemic communication plan, be sure to assess whether your plan is reliable; includes communication technology that addresses potential communication failures; has redundancy and overlapping message paths; sustains two-way and interactive communication; has high usability; is flexible and provides mobility capability; is verifiable; and enables you to communicate quickly, easily, and efficiently with large numbers of people in minutes, not hours.

See also Crisis Communication: External and Internal; Pandemics; and Risk Communication.

OUTSOURCING AND SECURITY

W. Timothy Coombs

Outsourcing is when management shifts noncore operations from internal production to an external entity that specializes in that operation. An outside vendor is contracted to handle what was once done internally at the organization. Organizations can outsource both manual and intellectual labor. Examples would include hiring a cleaning company rather than having a janitorial staff and having data entry performed by a vendor rather than an in-house team. Companies often outsource physical security by hiring private security firms. (Refer to the Security Guards/Officers entry for more information on this topic.) The main reason for outsourcing is cost savings.

A major downside to outsourcing is loss of control over those noncore operations. Part of the lost control is security. Outsiders now have access to information that could be sensitive, such as customer data. In 2005, Citibank had a case in which call center workers in Pune, India, stole $350,000 from customers. The workers secured the customers' passwords and transferred the money to fake accounts. The customers noticed the problem and brought it to Citibank's attention. Similarly, outsourcing payroll information can expose Social Security numbers so that they could be used in identity theft or other fraud.

The first concern in outsourcing security is to protect sensitive information. Security expert Bar Biszick-Lockwood recommends that organizations classify information and reconsider any outsourcing activities that would place sensitive information at risk. Sensitive information includes mission critical data, private customer information, private employee information, proprietary information, data used to calculate the organization's financial performance, and any data that would damage an organization if it were exposed. If you decide to outsource activities that involve this information, make sure the outside vendor can guarantee security.

The security issue on outsourcing is complicated further by governmental regulations such as the Sarbanes-Oxley Act. Such laws hold organizations accountable for actions that could be compromised by insecure information. Therefore, organizations must carefully vet their vendors for security. Generally, going offshore increases the risk in outsourcing deals because international law is weak at protecting intellectual property rights. For sensitive information, the recommendation is to keep the outsourcing within your national borders.

Make it very clear to vendors that security is a top priority and research their security efforts. It is appropriate to request an external security audit of the vendor. In addition, include a contract clause prohibiting the vendor from subcontracting or re-outsourcing the project, check contact information for other clients (references), review details on any recent security breaches and countermeasures taken to prevent their repetition, and ask the vendor to agree to U.S. jurisdiction.[1]

CONCLUSION

Outsourcing can result in cost savings for an organization. However, security should be a higher priority than cost savings. Organizations must evaluate each outsourcing project to determine the sensitivity level of the information associated with it. An organization should reconsider outsourcing any function that would involve highly sensitive information. Moreover, avoid outsourcing offshore if you do decide to outsource a project or function that includes sensitive information. Be sure to vet the vendor thoroughly for security concerns. Monitor the security risk throughout the entire outsourcing process. Ultimately, your organization will suffer the consequences if there is a security breach through your outsourcing. Customers blamed Citibank, not the call center, when money in their accounts was compromised.

See also Customs-Trade Partnership Against Terrorism; Information Security; Security Guards/Officers; and Supply Chain Security.

NOTE

1. Bar Biszick-Lockwood, “4 Steps to Secure IT Outsourcing,” online at http://www.sourcingmag.com/content/c050824a.asp (accessed 11 March 2007); Stephen Reed, “Managing Risk in Outsourcing,” online at http://www.sourcingmag.com/content/c051017a.asp (accessed 10 March 2007).

SUPPLY CHAIN SECURITY

W. Timothy Coombs

Supply chain security ties together ideas from many other entries in this work. In fact, this entry's "see also" list is one of the longest. A supply chain is the series of steps from the extraction of raw materials to getting finished products in the hands of consumers. These connections require a coordinated system of organizations, people, activities, information, and resources to move a product or service from supplier to customer. Every organization that comes into contact with a product is part of its supply chain. In a manufacturing organization, the typical supply chain includes organizations that manufacture the parts, assemble the parts, deliver the parts and products, and sell the products.

Today's business climate demands global supply chains to remain competitive. Organizations need to be able to access parts of their supply chain from anywhere in the world to help reduce costs. This is related to the market forces behind outsourcing. (See the Outsourcing and Security entry for security issues related to this practice.) Supply chains are multicountry and multivendor, and this trend is unlikely to change.[1] With long multivendor supply chains, it is critical that organizations collaborate for supply chain security. Supply chain security is complex, covering the areas of physical security, access control, personnel security, education and training awareness, procedural security, documentation processing security, information security, incident management and investigation, trading partner security, and conveyance security. The exact security concerns within these various areas depend upon the nature of your supply chain. This entry provides a generic overview of the security concerns involved in supply chains.

PHYSICAL SECURITY

Materials pass through various physical locations as they move through the supply chain. The physical security of each location needs be considered. There must be measures in place to monitor and control the exterior and interior perimeters of the various locations. Some key physical security concerns to consider are perimeter fencing, lighting of the perimeter, locking devices for internal and external doors, clear identification of restricted areas, restricted access to cargo areas, and oversight of all trash removal. Refer to the Physical Security entry for a more detailed discussion of the topic.

ACCESS CONTROL

Access control is often considered part of physical security as it covers access to facilities, conveyances, vessels, aircraft, shipping, loading docks, and cargo areas. The goal is to prevent unauthorized personnel from gaining access to materials as they move through the supply chain. Some key access concerns include being able to limit the access of people and vehicles, inspecting all vehicles entering and exiting access areas, enacting procedures for challenging unauthorized people, having people sign in and out of high-risk areas, restricting access to cargo storage areas, recording loading areas with CCTV, and installing alarms that can be sounded if unauthorized people enter a restricted area.

PERSONNEL SECURITY

Organizations must make sure the authorized people with access to materials in the supply are trustworthy. Personnel security involves the screening of employees and potential employees as well as being able to monitor employee access to cargo areas. Background and drug tests prior to and periodically after hiring are recommended. Color-coded identity cards and uniforms can be used to designate where an employee should have access. Biometrics can be implemented to limit access to sensitive areas. Refer to the entries Employee Background Screening and Drug Testing and Biometrics for further information on this topic.

EDUCATION AND TRAINING AWARENESS

Many entries have repeated the mantra that security is every employee's responsibility. To be effective, employees need to know and to understand security policies that are relevant to them. Education and training programs help employees with security policies, awareness of deviations from the policies, and knowing what actions to take when a violation does occur. The security policies and standards must be communicated to all employees. Incentives can be offered to employees reporting suspicious activities.

PROCEDURAL SECURITY

Procedural security involves efforts to record and verify the introduction and removal of materials from the supply chain. Supply chain partners must know when something enters or exits the supply chain. Written verification security procedures should be in place and shared with supply chain partners. Methods need to be established for identifying and verifying authorized carriers and authorized cargo. Guidelines are required for affixing, replacing, recording, tracking, and verifying devices used to ensure the cargo is authentic and has not been adulterated in some fashion. Such devices include seals, serialized tape, or radio frequency identity tags.

Procedural security also covers the proper storage of cargo, correct storage of empty containers to prevent unauthorized access, and checking whether empty containers received for storage have been altered. Employees should guard against unauthorized materials from entering the supply chain as well. All personnel and packages that can come into contact with the cargo should be searched, and the security devices such as seals stored securely.

DOCUMENTATION PROCESSING SECURITY

Documentation processing security tries to ensure that all information is legible and safe from exchange, loss, or falsification. All cargo should be recorded, including packing condition, unit type, and security devices. The people logging in cargo must provide printed names and signatures. Investigate any deviation from the reporting process. Record the entrance and exit time of people receiving and delivering goods. Put special control processes in place for emergency or last-minute shipments. The documentation processing security must be responsive to the special needs of emergency shipments.

INFORMATION SECURITY

Information security seeks to protect the integrity of information about the supply chain against loss, exchange, and introduction of false information. Supply chain information should be available only to those who need to know and procedures in place to keep the information away from unauthorized personnel. This includes physical and information security for computer systems. Refer to the Information Security entry for more information on this subject.

INCIDENT MANAGEMENT AND INVESTIGATION

Incident management and investigation cover the tracking and information coordination capability of an organization with the purpose of timely reporting missing or lost cargo. The point of supply chain security is to make sure cargo arrives when and where it is intended. Supply chain partners need to know when cargo has gone missing and how the loss will be investigated.

TRADING PARTNER SECURITY

An organization must be sure the concern for supply chain security extends to and is shared by its suppliers and customers. Trading partners should agree to security procedures, even to the point of writing them into contracts. Key activities include requesting supply chain partners to assess supply chain–related security, using seals or other security devices, and documenting supply chain security policies. Coordination is central to trading partner security. Trading partners must share security-related information, share educational and training materials, and work together to identify, prioritize, and address supply chain security concerns.

CONVEYANCE SECURITY

Conveyance security seeks to protect against the introduction of unauthorized personnel or materials into the supply chain. Security devices and procedures and access control all help to protect conveyance security. High-risk cargo should be given special consideration. For instance, using two drivers, escort services, driver security training, and varied routes are examples of special considerations. Clearly conveyance security overlaps all of the other elements of supply chain security in this entry.[2]

CONCLUSION

Organizations will find a continuing and growing need to address supply chain security because the trend is for supply chains to have more links and links that have greater geographic diversity. Supply chains challenge supply partners to create a secure environment for the storage and transportation of cargo. A number of security concerns and organizations must converge to craft an effective supply chain security program.

See also Biometrics; Supply Chain Continuity; Customs-Trade Partnership Against Terrorism; Employee Background Screening and Drug Testing; Information Security; Outsourcing and Security; Physical Security; Radio Frequency Identity; and Terrorism.

NOTES

1. Kenneth Karel Boyer, Markham T. Frohlich, and G. Tomas M. Hult, *Extending the Supply Chain: How Cutting-Edge Companies Bridge the Critical Last Mile into Customers' Homes* (New York: AMACOM, 2005), pp. 1–23.

2. "C-TPAT Security Guidelines," 2006, online at http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/security_guideline/ (accessed 5 March 2007).

SUPPLY CHAIN CONTINUITY

Geary Sikich

Cargo security is a problem for industry. Annual losses due to cargo theft run between $10 billion and $15 billion. According to the National Cargo Security Council (NCSC), motor carriers are the victims in 85 percent of all cargo theft, the majority taking place at terminals, transfer facilities, and cargo consolidation areas. However, these statistics may not reflect the actual situation. The FBI reports that only 40 percent of businesses or individuals actually report theft. If indirect costs are factored in, total losses are estimated to be between $20 billion and $60 billion a year.[1] Cargo safety is but one of the problems that can befall a global supply. Business continuity planning must extend beyond a business to the members of its supply chain.

No one company can deliver products and/or services end to end in today's complex business environment. Your company, like other companies, is most likely dependent on vendors of various types (manufacturing, professional services, software, transportation, etc.) to meet customer expectations.

All the people and organizations involved in getting product to market make up a supply chain. Because a supply chain is typically a mix of competencies, it poses a risk to an organization. That's why developing a process for ensuring business continuity throughout the supply chain is important. An interruption in your supply chain could mean a major disruption to your company.

Effective business continuity strategies, such as supply chain assurance, need to be designed. This entry discusses the process for building business continuity capabilities into the supply chain. The first section considers how to examine the supply chain to ensure business continuity in the face of trouble. Figure 1, Supply Chain Business Conituity, provides a visual summary of business

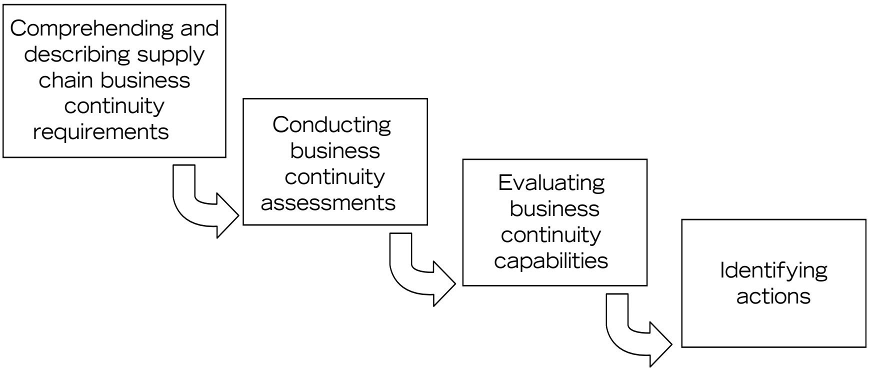

Comprehending and describing supply chain business continuity requirements
Conducting business continuity assessments
Evaluating business continuity capabilities
Identifying actions

Figure 1 Supply chain business continuity elements.

continuity and the supply chain. The second section discusses how to integrate business continuity into the supply chain using the procurement process as a guide. The third and final section reviews the need for early identification of problems through incident management.

ASSESSING A SUPPLY CHAIN FOR BUSINESS CONTINUITY CONCERNS

Developing and implementing criteria for assessing the business continuity capabilities of vendors operating within your supply chain can be a daunting task. The scope of activities involves assessing current procurement processes, first by collecting and analyzing data and then by making the necessary changes to the procurement planning. This may include determining a vendor's ability to maintain supply chain continuity in the face of disaster, economic trouble, or other challenges; developing assessment processes; defining contract terms and conditions; developing sustainability procedures; and making business continuity an integral component of your procurement process.

It is helpful at this point to review the risks that can impact an organization's supply chain. These risks can be articulated as either internal or external, as depicted in Figure 2, Internal and External Vulnerability Drivers.

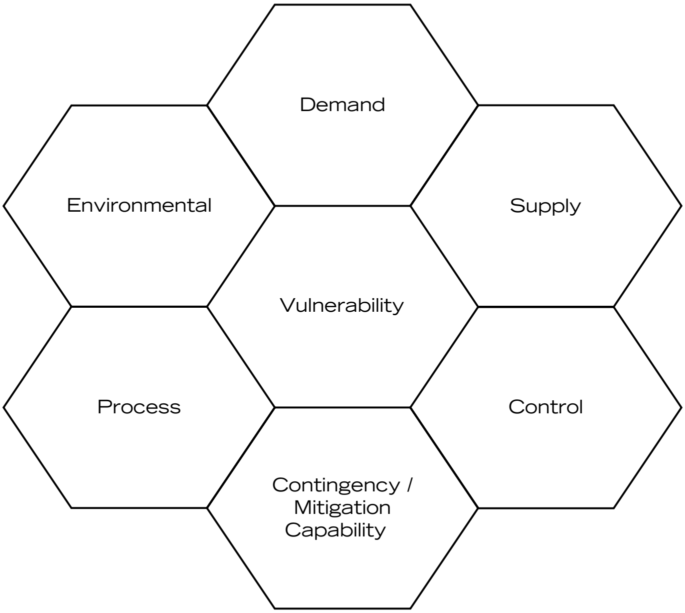


Figure 2 Internal and external vulnerability drivers.

These drivers and the ability to manage them—by putting contingency measures into place—often are interconnected. Understanding this potential interconnectedness helps in assessing vendor business continuity capabilities. Internal and external vulnerability drivers can materialize in a variety of ways. Risk can be context sensitive, as risk elements interact differently depending on the situation. Understanding the potential interaction of risk factors facilitates measuring business continuity capabilities and planning for actions that can be implemented should a disruptive event occur.[2]

Vendor Continuity Capability Questionnaire

The first action to take when assessing the supply chain for business continuity is evaluating current practices of vendors in the supply chain. Developing a vendor continuity capability questionnaire is a good first step but needs to be carefully thought through. You are, in essence, creating a legal document that could contain sensitive information that must be protected. You are also creating a potential liability document for yourself. With the type of information collected to assess vendor continuity capabilities, your organization could be held liable under the concepts of negligence (foreseeability), constructive notice, and/or constructive knowledge, for *not* taking action to mitigate potential losses.

The structure of a typical eight-part vendor continuity capability questionnaire is summarized below:

Part 1: Governance Provisions and Management Commitment
The purpose of this part of the questionnaire is to establish that the vendor has a formal governance program in place that has management commitment. You also want to ascertain whether the vendor's program is integrated into the way it does business or is an adjunct to the business that it is in.

Part 2: Business Continuity Strategies: Developing and Implementing BCP
The purpose of this part of the questionnaire is to gain an understanding of the vendor's strategy for continuity in the face of trouble and how it will implement the business continuity plan (BCP).

Part 3: Business Impact Analysis, Risk Evaluation, and Control Mechanisms
Part 3 of the questionnaire seeks to gain an understanding of the extent to which the vendor assesses possible negative impacts and how often; identifies and evaluates risks; and institutes control mechanisms to address risk and mitigate threats, hazards, and overall vulnerability.

Part 4: Maintaining Continuity: Training, Awareness, Exercises, and Business Continuity Plan Updates
This part of the questionnaire seeks to gain an understanding of the extent and adequacy of the vendor's continuity program training and whether it updates its plans regularly to take advantage of new situations and information.

Part 5: Incident Response Operations
Part 5 looks at the tactical level of business continuity with the goal of understanding how the vendor identifies, responds to, and communicates information on disruptive events.

Part 6: Crisis Communications
Part 6 focuses on the vendor's internal and external communications relating to policies, information flow, and the management of crisis communications.

Part 7: Coordination (External Entities)
Part 7 of the questionnaire is designed to assess vendor coordination with external parties, including the government, customers, and its own vendors. It also assesses key components of the coordination process.

Part 8: Vendor Certification
The final section asks the vendor to certify the accuracy of the answers on the questionnaire.

The exact questions and the length of the vendor questionnaire will vary depending on the industry and the depth of analysis that you want to perform. The questionnaires that I have developed for clients contained approximately fifty questions that require the vendor to provide quantifiable answers. Should you determine the need for further analysis, assemble a formal audit team to resolve the concern over vendor continuity capability.

Vendor Continuity Capability Assessment

During the course of assessment, data will be collected, analyzed, and developed into findings and recommendations. The data should be organized by essential element of analysis (EEA) criteria that the organization establishes and uses to conduct data collection, analysis, and evaluation. Examples of typical EEA are provided in the Essential Elements of Analysis box.

Essential Elements of Analysis

Organization

This refers to the current procurement process, vendor roles/responsibilities and deliverables during the procurement process life cycle, and current criteria for the organization's business continuity programs and plans. Evaluation issues include, but are not limited to, determining the following:

- Whether continuity is a strategic consideration for the vendor that results in specific ways of doing business or is an adjunct to the vendor's business

- Where in the vendor organization ownership of the business continuity program and plans resides
- To what extent the vendor's senior management team gets involved in the vendor continuity program

Vulnerability Identification and Control

This refers to establishing minimum acceptable criteria for vendor vulnerability identification and control methodologies. The purpose is to maintain continuity programs and allow the vendor to integrate its methodologies on a sustainable basis with the client's business continuity management strategy. Topics assessed include the following:

- Vendor methods for identifying and assessing threats, hazards, vulnerabilities, and risks
- Vendor methods for determining risk acceptance levels
- Vendor validation methods for assessing response, management, and recovery capabilities
- Vendor methods for integrating methodologies with current business impact assessment efforts

Continuity Strategy and Approach

This refers to the measures developed and used to verify vendor integration of the business continuity management program and plans with the client's business continuity management strategy. Assessment includes the following:

- Vendor methods for determining critical business functions and requirements
- Vendor compliance with minimum acceptable criteria for the business continuity management program and plans
- Vendor monitoring and enforcement of compliance across the business continuity management program and plans

Documentation

This refers to the documentation of vendor business continuity management program and plan capabilities. Key issues include the following:

- Policy, plan, and supporting documentation
- Measures

(continued)

- "Value chain" integration
- Communications (internal, external, including media and stakeholder handling)
- Vendor verification of integrated response, management, and recovery capabilities and documentation

Resource Management and Development

This refers to the metrics for vendor validation of staffing (business continuity staffing) and associated vendor integration of continuity planning, resource development, and awareness of continuity. Areas audited include the following:

- Vendor personnel, funding, expert knowledge, and future requirements to support the program and when they will be needed
- The functional roles and responsibilities of vendor organizations, departments, and individuals in support of business continuity management
- Vendor program, protocols, and effectiveness
- Vendor knowledge transfer and integration
- Vendor training and simulation activities
- Vendor facilities and equipment program status

Continuity Maintenance

This refers to the procedures used to ensure resilience of the vendor continuity process. Key areas audited include the following:

- Vendor maintenance protocols and effectiveness
- Vendor change control protocols

PROCUREMENT PLANNING CONSIDERATIONS

The overall objective of integrating business continuity criteria into the supply chain is to make the procurement process more efficient and safer from disruption. Once you determine what is needed, the focus shifts to addressing weaknesses through procurement planning. With any large-scale project, such as the integration of vendor business continuity criteria into the procurement process, attempting to implement on a grand scale can lead to chaotic results. A phased approach to implementation and integration is a better idea and should generally consist of five phases:

- *Phase 1:* Assessment and vendor continuity questionnaire—deliverable: letter report with executive summary that will include discussion and recommendations based on the results of the review of essential elements of analysis (report)
- *Phase 2:* Procurement integration (vertical/horizontal)—deliverables: procurement management system, vendor business continuity management program, and plan integration criteria guide (tools), and training program materials for each (knowledge transfer)
- *Phase 3:* Monitoring and enforcement—deliverable: procurement management system, vendor business continuity management program, and continuity plan integration criteria guide maintenance criteria (sustainability)
- *Phase 4:* Sustainability—deliverable: periodic metrics, event response reports
- *Phase 5:* Maturity model evaluation—deliverable: metrics for maintaining the process, change management procedures

PROCUREMENT INCIDENT MANAGEMENT CONSIDERATIONS

A vendor can complete the vetting process and still experience a disruption affecting your company's ability to meet customer demand. Problems will occur, and the sooner these are detected, the sooner they can be resolved and the better an organization can protect its assets. Having an incident management system as a component of the procurement process can allow your company to respond, recover, and restore supply chain operations with less potential for massive disruption. Incident management can range from assessing and classifying a vendor incident to implementing response actions, such as sending your personnel to vendor facilities to assist in incident mitigation processes.

Contingency alternatives can range from having backup response plans to alternative sources of supply. Once the risks are identified and evaluated, actions to address them throughout the procurement process can be taken. Identifying risk themes across a number of risk dimensions can help to determine where your company should place effort to mitigate the risk exposure.

Disruptive events as they occur need to be classified by their level of severity in order to determine their potential impact. Figure 3, Disruptive Events, offers an example of a classification system for disruptions. A classification system can provide a consistent framework for evaluation; enhance the communication process between internal and external groups; and facilitate response, management, recovery, and restoration efforts.

Consider creating an event assessment form to use in conjunction with the event classification system for determining the event classification level and for

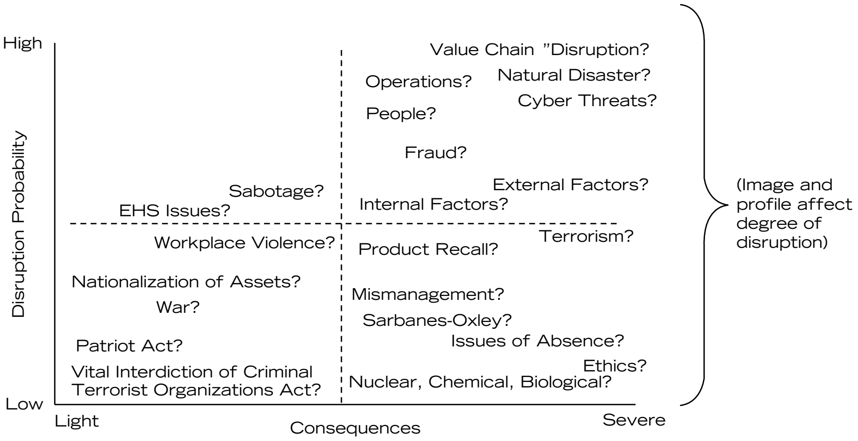


Figure 3 Disruptive events.

facilitating discussion within your company and with the affected vendor(s). The less prepared an organization is for service disruption, the longer it takes to recover operations and restore service levels. Having a classification system can help in identifying potentially disruptive situations early and determining how to respond effectively to minimize the level of service impacts.

The procurement process represents the first line of direct contact with vendors, suppliers, and so on. The ability of procurement personnel at any stage of the procurement cycle to detect and classify potential disruption and severity allows your company to implement its business continuity plan and coordinate with affected vendors to assure continuity of operations. Early detection, classification, and response can also help keep service at a high level, reduce potential chaos associated with a disruptive event, and lead to shorter recovery and restoration time frames.

CONCLUSION

Assuring supplier continuity capabilities is of paramount concern today. Realizing that most business processes extend beyond the boundaries of a single entity, businesspeople are more aware of critical supply chain interdependencies. Simply having profiles of potential high-risk suppliers, while extremely important, is by itself not enough. You need to develop capabilities to assess and monitor vendors to identify potential problems before they occur.

Business leaders have the responsibility to protect their organizations by facilitating continuity planning and preparedness efforts. Senior management and board members can and must deliver the message that survivability depends on being able to find the opportunity within the crisis. Today, we cannot merely think about the plannable or plan for the unthinkable, but we must learn to think about the unplannable. Market research indicates that only a small portion (5 percent) of businesses today has a viable business continuity plan, but virtually 100 percent now realize they are at risk. Seizing the initiative and getting involved in all the phases of crisis management can mitigate or prevent major losses.[3]

See also Business Continuity; Customs-Trade Partnership Against Terrorism; and Supply Chain Security.

NOTES

[1] Sean Kilcarr, "Cargo Theft a Growing Threat," 10 Oct. 2002, online at http://driversmag.com/ar/fleet_cargo_theft_growing/index.html (accessed 23 April 2007).

[2] Lord Levine, "Changing Risk Environment for Global Business," 8 April 2003, online at http://www.lloyds.com/NR/rdonlyres/E3A3A19D-F459-4D76-8677-CD3E89EE43F5/0/LordLeveneSpeechcostoflitigation2003.pdf (accessed 10 April 2007).

[3] Geary W. Sikich, *Integrated Business Continuity: Maintaining Resilience in Times of Uncertainty* (Tulsa, OK: PennWell Publishing, 2003).

TRAVEL OVERSEAS

W. Timothy Coombs

When businesspeople travel, especially overseas, they must address some of their own security concerns. Companies should provide training to make employees aware of key security issues when they travel. Security measures must be taken to ensure personal safety as well as security of sensitive or proprietary company information in their possession. Overseas, personnel are at risk of criminal and terrorist acts. (The Terrorism entry outlines the basic terror groups and their geographic range.) This entry is divided by the elements of the travel process and emphasizes the need to be aware of one's environment.

TRAVEL PREPARATION

Research or be briefed on the country you will be traveling to. Check with the U.S. State Department for any travel warnings for that country or region of the world. Do not pack any sensitive or proprietary information; keep that with you in your carry-on luggage. For extra security, double envelope the material. Select luggage tags that have a cover and do not use laminated business cards for luggage tags. The objective is not to advertise your country of origin or company's name. Avoid exchanging currency in public areas of the airport that are targets for criminals. It is advisable to exchange some currency before you leave or to exchange currency before leaving the secure area of the airport. Make sure you will be flying through secure airports, even on layovers. Again, the U.S. State Department has information on the level of security at various international airports. Wide-body planes are less attractive targets for terrorists, although aisle seats place you closer to the action and at greater risk if there is a hijacking. Dress in casual clothes to draw less attention to yourself.

AT THE AIRPORT

Try to avoid long lines at the airport by arriving early for check-in. Pack for security ahead of time; do not repack your bags at the airport. Check with the Federal Aviation Authority (FAA) for the latest guidelines on carry-on luggage. This will help you to avoid problems at security checkpoints. Keep in mind that regulations are not the same in every country. As always, keep your luggage in sight at all times. When possible, use a hotel vehicle for transportation to and from the airport. If that is not possible, use “official” transportation. Always be vigilant for suspicious activity and people. Avoid open public areas, especially those with a lot of glass, which are inviting targets for bomb attacks.

AT THE HOTEL

Before you book your stay, check on the security level of your hotel. One way to do this is to contact the regional security officer at the local U.S. embassy for a list of hotels that government officials use when visiting. The best option is to stay at a hotel that is part of a U.S.-based chain. It will have security standards consistent with those in the United States. Parking garages are the most dangerous places because they are difficult to secure. In the lobby, notice if anyone seems overly interested in your arrival. Have a hotel staff member take you to your room and make sure the room is empty. Inspect the security features, such as locks, before the hotel employee leaves. Review the safety features such as where the nearest fire exit is located as well as the nearest house phone. Check and verify when hotel staff requests entry to your room. Criminals can use pretexting, pretending to be an employee, to gain entry. Use the optical viewer to determine whether the person has the proper uniform, and call the main desk to confirm someone was sent to your room.

Never discuss sensitive or proprietary information while in your hotel room because it may not be secure. The same goes for using the telephone in your room. Keep your key and passport with you at all times. Do not jog or walk in cities or areas you do not know well. Vary the times you leave and return to the hotel. Keep valuables in a secure location such as a safety deposit box at the main desk.

Exercise caution in and around public restrooms at the hotel, a prime location for criminal activity. Keep your hotel door closed and the deadbolt locked when in your room. Be sure the door closes fully and locks when you leave your room.

DRIVING A CAR

Many business travelers like to rent cars for local transportation. When you rent a car, make sure to choose a vehicle that is common in that location. And, if possible, ask that the rental company remove any markings signaling the vehicle is a rental. You should be trying to blend in with the other cars so that you do not become an obvious target. Air-conditioning is a good idea to prevent rolled-down windows, which are a safety risk.

Here are some other car safety points people should follow in any city: avoid driving at night, keep your doors locked at all times, wear a seat belt, do not leave valuables in the car, do not park on the street overnight, and do not pick up hitchhikers. Be smart about how and where you drive. This will serve to maximize your safety when you feel you must rent a car for transportation.

TRAIN TRAVEL

Train stations have open access and are targets for criminals and terrorists. Be very vigilant when using these facilities. Trains are inviting targets for bombings and sabotage as well. They are considered “soft” targets because they are easy to access. Trains travel over miles of tracks that are simple to target.

TARGETING RECOGNITION

We hate to think the worst of people, but that is a useful trait when it comes to personnel security. Be suspicious of people who act that way. Here are some examples of suspicious behavior:

- Repeated contact with the same person who is not a business contact
- A business contact who tries to push the relationship beyond business
- Accidental meetings whereby a person then tries to strike up a conversation by practicing English, asking about your employer, or wanting to buy you a drink

These may be innocent encounters or else someone is targeting you for theft or kidnapping. Be alert and suspicious, especially when traveling in a high-risk country or area. If you think you are under surveillance, watch what you say. Do not try to give someone the slip; do not search your room for listening devices.

These actions send the wrong signal to surveillants. Report any suspicions to the U.S. embassy and follow its recommendation.[1]

CONCLUSION

Most of personal security while traveling is common sense or points we have heard announced to us numerous times over the airport public address system. The key is planning, preparation, and common sense. For more detailed information on personal security overseas, read the U.S. State Department's "Personal Security Guidelines for the American Business Traveler Overseas," included in the Document Appendix.

See also Countersurveillance; and Terrorism.

NOTE

[1] "A Safe Trip Abroad," 22 Jan. 2007, online at http://travel.state.gov/travel/tips/safety/safety_1747.html?css=print (accessed 3 Feb. 2007).

CORPORATE OR INDUSTRIAL ESPIONAGE

W. Timothy Coombs

The U.S. government does track attempts by foreign agents to acquire sensitive information. The focus is on military-related technology. However, government reports also document efforts to acquire economic-related technology that provides companies with a competitive edge. Annually, agents from nearly one hundred countries attempt to procure what is classified as sensitive U.S. technology. Companies should realize they may be targets of foreign agents seeking sensitive technology. Frequent targets are companies involved in semiconductor production processes, computer microprocessors, software, and chemical processes. The government has documented that U.S. companies that lose sensitive information experience a decline in investor confidence and stock price. This is one form of corporate or industrial espionage, defined as illegal or unethical efforts to collect information for commercial gain rather than national interests. Examples of corporate or industrial espionage include bribery, theft, blackmail, technological surveillance, and violence.

U.S companies are attractive targets for foreign agents because of the openness of the United States to visitors. Many companies and universities employ foreign workers, who often have the skills necessary to acquire technology illegally. Companies may host foreign visitors as well for short-term or long-term visits.

Visitors may try to secure information by engaging in conversation and asking about the technology, by sneaking into areas where they can view or access sensitive information, or by trying to circumvent security. Long-term visitors are a greater risk than short-term visitors. A long-term visitor has more of an opportunity to learn the security procedures and devise ways to circumvent them. Information security is at the greatest risk. A long-term visitor has time to acquire passwords and can learn where sensitive information is stored. Short-term visitors are easier for people to see and to observe, whereas long-term visitors begin to blend in with other workers and are given less scrutiny. Technology, such as small portable storage devices with large capacities and picture phones, is another factor making it easier to engage in industrial espionage.[1]

Electronic storage devices that employees take abroad, such as laptop computers, personal digital assistants (PDA), and cell phones, are another source of risk. A recent survey found that over 66 percent of U.S. businesspeople carry

Corporate Espionage Case Study: KPMG

KPMG is a consulting company that provides a variety of business services, including financial services. Guy Enright worked as an accountant for KMPG in its Bermuda office. In May 2005, he was contacted by a man claiming to be a British secret agent named Nick Hamilton. Agent Hamilton claimed KPMG had information vital to national security interests in Britain. Hamilton wanted financial audit information about IPOC, a client of KPMG's. Enright agreed to provide the information, and the plot of a spy novel ensued. Enright left documents for Hamilton in a number of clandestine locations, including the storage compartment of a moped.

The problem was that Nick Hamilton was not an agent for the British government. Instead, his real name was Nick Day and he was the cofounder of Diligence Inc., a private intelligence company located in Washington, DC. Its advisory board includes former major politicians from both the United States and the United Kingdom. Diligence Inc. was working for a company named the Alfa Group Consortium, hired through the powerful lobbying firm of Barbour Griffin & Rogers. The Alfa Group Consortium was in competition with IPOC for a lucrative stake in the Russian telecom company MegaFon.

Business Week printed a lengthy story about the espionage incident. Diligence Inc. labeled the operation project Yucca.

(continued)

Memos from Diligence Inc. claimed there was virtually no chance of being detected and that their actions would maintain plausible deniability. Diligence Inc. first collected a list of names of the people in the KPMG Bermuda office. Enright was carefully watched to be sure he was not a plant or a corporate spy himself. Project Yucca ended when an unknown source left a collection of records and e-mails about the project at the New Jersey offices of KPMG. KPMG filed a lawsuit against Diligence Inc. in U.S. District Court in November 2005. Diligence Inc. settled in June 2006 for $1.7 million. IPOC has sued both Diligence Inc. and Barbour Griffin & Rogers.[2]

The actions of Diligence Inc. crossed the boundary from competitive intelligence to corporate espionage. Nick Day's posing as a British secret agent was definitely unethical and possibly illegal. Blatantly lying about one's purpose and organization falls well outside the realm of competitive intelligence, which prides itself on using ethical and legal means to obtain information.

important company information on their PDAs. Electronic storage devices can be compromised or stolen from hotel rooms or at security checkpoints.[3] Some PDAs can even be compromised/accessed remotely. See the entries Portable Device Security and Travel Overseas for ideas on securing data on electronic devices and security while traveling. Travel for conventions, expositions, and trade shows creates special problems. If your company is an exhibitor, it is a target. Hotels can be searched for sensitive information including technical reference manuals. Be sure all such information is secure at all times in all locations. The KPMG case is reminder that corporate espionage is real.

Foreign agents do not have to rely on cloak-and-dagger techniques to gather sensitive information. The most common strategy is simply to ask for the information through e-mail, by fax, or in person. The foreign agent often builds a relationship through conversations with an individual at a company before making the request. One strategy is to pose as a graduate student conducting research. The "fake" graduate student converses with a scientist about his or her work. When the time is right, the request for sensitive information is made and many times the scientist provides it; the graduate student seems to be a friend who is simply interested in research. Employees should be reminded not to share sensitive information with anyone, period.

Another common access point is via the Internet, one more reason companies must be concerned about cyber security. Refer to the entry Information Security for recommendations on protecting a company from cyber attacks. No system can be made perfectly safe from cyber attacks, but security should be better than it is at most companies. Consider a recent survey that found nine out of ten companies had serious Internet vulnerabilities when the companies believed they were extremely secure.

Finally, the foreign agents are not just government operatives. Government statistics indicate the largest classification of foreign agents trying to gather sensitive information is private companies at 36 percent. Those working for a government represented 21 percent, with another 15 percent being affiliated with a foreign government. Keep in mind these statistics do not include domestic activities. Competitors in the United States can be trying to extract sensitive information from a company as well. The techniques for collecting the information remain the same; only the names of the actors seeking the information changes.[4]

CONCLUSION

If your organization handles sensitive technology, assume that you are a target for foreign agents trying to acquire that technology. Carefully monitor all visitors to your facilities whether they are short-term or long-term visits. Review basic cyber security and electronic storage device security with your employees. Emphasize the danger presented when traveling with laptops and PDAs. Finally, warn your employees about the common strategies foreign agents use to trick employees into divulging information. Having strong security policies and creating awareness among employees are critical to preventing corporate/industrial espionage.

See also Competitive Intelligence; Countersurveillance; Information Security; Portable Device Security; Social Engineering: Exploiting the Weakest Link; and Travel Overseas.

NOTES

1. Office of National Counterintelligence Executive (ONCIX), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2004*, April 2005, online at http://www.fas.org/irp/ops/ci/docs/2004.pdf (accessed 10 March 2007), pp. ix–xi.

2. Eamon Javers, “Spies, Lies & KPMG,” *BusinessWeek,* 26 Feb. 2007, pp. 86–88.

3. “Confiscated Laptops,” *Security Management*, Feb. 2007, p. 44.

4. ONICIX, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*—2004, pp. 1–7.

ENHANCING THE HUMAN SIDE OF SECURITY AND SAFETY

A common theme through most discussions of security and safety is the central role of people. If people fail to follow policies or execute desired behaviors, security, safety, or both can be compromised. This section provides general advice on how to improve the human side of security and safety.

IMPROVING TEAM EFFECTIVENESS

W. Timothy Coombs

Teams are often a part of business continuity, security, crisis management, and disaster recovery efforts. A number of the entries in these two volumes mention the use of teams to create various plans and policies for organizations. Moreover, teams are expected to execute various response plans when trouble arrives. Although we put a lot of faith in teams to succeed, we often fail to provide an environment in which this can happen. Our own mistaken assumptions about teams create the negative environment for teams. By exposing these common mistaken beliefs, we gain insights into the training needed to make teams effective and help them to succeed.

PROBLEM ASSUMPTIONS ABOUT TEAMS

Assumption 1

If we put people together on a team, they will work as a team. People are not born knowing how to function as a team. In fact, in the United States, our culture works against teams because we value and praise individual effort. This is reinforced in the workplace with rewards systems that focus on individual rather than team performance. We are not "wired" to be effective team members, so training is needed to form teams that work.

Assumption 2

Teams are always better than people working alone. It is true that a "synergy" occurs when people form teams. The interaction of people creates something unique from the sum of individual efforts. However, unique does not necessarily mean better. Teams can still make mistakes and ineffective decisions. Effective decision making requires training; it does not happen by chance.

Assumption 3

Select the best employees and excellence will follow. The belief is that if we place the best and brightest employees on a team, the team will perform at a high level. However, these are the people most likely to value and have benefited from individual effort. The best individual performers are not necessarily the best team performers. The skills to do your job may not be the same skills needed to function as a team.

These mistaken assumptions combine to blind us to the need to train people to be team members. We cannot assume people know how to function in teams or that they learned it somewhere else. Even our top people must be trained on key team skills if we are to have effective teams. This leads to the second point, the training necessary to develop effective teams.

DEVELOPING EFFECTIVE TEAMS

A team is a group of individuals that works together to perform tasks. People on a team need to take some actions on their own and some in coordination with others. For teams to work, people need both individual-level and team-level competencies. People must be responsible for their own actions as well as the welfare of the team.

Individual-level competencies center on contributing to the team. A person is placed on a team to contribute. He or she has unique knowledge and skills that can help the team. The benefits a person can provide a team are lost if that person does not contribute to the team. Contributing means a person is willing to share his or her ideas and opinions by speaking up in a team setting. Training must encourage people to participate in the life of the team by reinforcing the value of individual contributions. It should be noted that in rare cases some people have extreme phobias about communicating in a team. Those suffering from such anxieties should not be placed on teams. The average person may be a bit anxious about expressing him or herself, but training can help to reduce that apprehension.

Speaking up on a team is linked to listening. We all think we are good listeners. However, a number of factors work against effective listening. Our minds work quicker than people can speak. As result, we can distract ourselves when listening to others by thinking of something else. Our mind's extra processing time can result in us drifting off. We must learn to stay focused. Also, we tend to dismiss or ignore ideas that are different from our own. We must learn to listen to all perspectives. Part of effective listening is trying to understand the point of view of each person speaking.

Team-level skills center on the decision-making process. The central deliverable of a team is its decisions. In fact, we typically judge team effectiveness by its decisions. Have you ever been trained in team decision making? Again, it is dangerous to assume teams know how to make decisions. Teams are unsuccessful at decision making for three reasons: failure to analyze the problem, failure to develop decision criteria, and failure to evaluate decision options carefully.

A team starts a decision by determining the problem it faces. Ineffective teams assume they know what the problem is and jump to solutions. Team members may think the situation looks like a problem they've handled before or want it to be so. The result is the team solves the wrong problem! Start by reviewing the situation to determine the real problem. Ineffective teams may have no criteria for evaluating decision options. As a result, they pick the one that sounds best or is pushed by the most powerful person on the team. Finally, ineffective teams do not evaluate their decision options carefully. If you have not developed decision criteria, you cannot effectively evaluate decision options. However, even teams that develop criteria may not apply them. The team does not carefully assess each decision option against the decision criteria to see which one is the best fit. Again, the selection is based on some preference unrelated to the effectiveness of the decision options.

Any one or combination of the three decision errors can sink a team. Teams need to be trained on proper decision-making techniques. This does not have to be a major training effort; it can be done in a few hours. People learn the common problems and strategies for overcoming those problems and then apply those newfound skills by practicing team decision-making tasks. The end result will be teams that are less likely to make the three common decision errors.

Part of decision making and life on a team is conflict. Disagreements can arise over the definition of the problem, decision criteria, evaluation of decision options, or where to order lunch. Conflict can be positive for a team. Airing multiple viewpoints helps a team to see the problem better and to evaluate the decision options. However, conflict can be destructive if handled negatively. Conflict needs to center on ideas, not personalities. People should be trained in the basics of conflict management, including the different styles for approaching conflict and the differences between productive and injurious conflict. Proper conflict management is a skill that benefits people in their regular jobs as well as in team activities.

CONCLUSION

One factor that effective teams have is their belief that they can handle any task; this is known as team potency. Training feeds into team potency by setting the stage for team success. By training on individual-level and team-level competencies, the team gains the skills necessary to succeed and to build confidence in its abilities. We entrust teams with important tasks, such as developing and implementing business continuity plans. Avoid the dangerous assumptions that lead to the belief that people naturally work effectively together as a team. Spend the time to train your teams to maximize the likelihood of their success.

See also Business Continuity; Crisis Management; Crisis Management Team; Disaster Recovery Management; and Benefits of Emergency Management.

AVOIDING THE SILO EFFECT TO IMPROVE BUSINESS SECURITY

Betty A. Kildow

An all-too-common condition in both government and private organizations today is business units that seem to operate almost autonomously with little understanding of what other departments are doing and how they impact one another. If we consider the silos used in farming for more than 130 years, it is not difficult to see how the term *silo effect* came to be. Although silos can be located next to or near one another, silos are soundproof, and people inside silos are unable to communicate with those on the outside. It’s dark in a silo, and its closed environment allows for little fresh air.

WHY SILOS EXIST

In business, silos almost exclusively value their own business functions, needs, and interests with little appreciation for the contributions of other business units. These silos may be formed by intent or default—without realizing that is what is happening (ignorance) or because “that’s the way it is here” (accepting and at times expanding the status quo).

Silos exist for a variety of reasons: a perceived means of building or maintaining power, politics, turf protection, history, and specialization of tasks. Simply put, silos are self-contained departments or other business units that struggle when communicating or working with other departments or silos. Large, complex organizations are a natural building site for silos, and silos are also easily created whenever two or more organizations merge—by whatever process.

DANGERS OF SILOS

The existence of silos in organizations significantly debilitates effective communication and productivity. The duplication of effort due to interdepartmental tension is at times astounding. In some organizations, silos are deliberately built and encouraged by upper management to create what is seen as "healthy competition." However, the lack of effective interdepartmental communication has proven time and again to be the undoing of effectiveness, and the existence of strong silos will almost assuredly negatively impact the end results.

These disconnected units, silos, become multiple organizations within an organization, focusing inward. Silos often store information that can be accessed only by either those within the silo or those with control or credentials deemed to qualify the holder for need-to-know status. Communication tends to be vertical, making timely coordination and communication among business units difficult, if not impossible. True collaboration becomes increasingly difficult. There is no sharing of resources. In some organizations, getting work done cross-functionally can be difficult at best, impossible at worst.

This can lead to reduced productivity, possible duplication of effort, and even tension and mistrust within the organization.

The "right hand not knowing what the left hand is doing" can result in a lack of valuable information sharing between business units, in losing sight of the goals of the organization as a whole, and in extreme situations by creating an "us" versus "them" mentality or turf wars (covert or overt). In addition, silos do not stand up well against high winds, such as the quickly changing requirements of responding to threats to the organization's security or dealing with emergencies and disasters.

That being said, it is possible that silos have value in some environments, such as where security of highly sensitive information is important or in short-cycle projects with a narrow mission.

SILOS AND EFFORTS TO PROTECT ORGANIZATIONS

There continues to be a growing awareness of silo mentality and its harmful impact, and those of us involved in keeping our organizations safe, secure, and operational are not necessarily immune. In some large organizations, a multitude of business units, such as those involved in business continuity (BC) and disaster recovery (DR), emergency management, security, crisis management, safety, environmental health and safety, and perhaps others, has shared responsibility for addressing risks, possibly leading to both planning gaps and overlaps. We would do well to learn from the mistakes of others.

The disciplines charged with keeping the organization's people, operations, and facilities safe and functioning do span silos. For example, effective business continuity planning follows, examines, and tracks the entire organization's operations, not only internally but also externally (e.g., suppliers, contractors, regulatory agencies).

That is not to say that for multiple reasons we have not collectively already developed our own silos, or at least laid the foundation for them:

- As the "new kids on the block" getting varying levels of respect and acceptance, we circled the wagons and began silo construction.
- Our language is "foreign"—between both us and them and us and us (public vs. private sector, aforementioned functions such as safety, security, etc.).
- Many organizations are not quite sure where some of the newer disciplines—disaster recovery and business continuity, in particular—"fit" in the organization, and as a result new silos are established.
- Historically, security, business continuity, disaster recovery, emergency management, and so forth have been segregated in individual departments, creating isolated silos.
- Disaster recovery practitioners in particular bear the scars of Y2K, as those who look back and put Y2K into the technology hoax category say, "I told you so," rather than considering the possibility that the blood, sweat, and tears that went into Y2K planning is the reason that the arrival of the new millennium did not create significant problems.

Although BC/DR is an organization-wide issue, there is a tendency on the part of people not directly involved in the planning process to believe that business continuity and disaster recovery are separate from the rest of the organization, "something that Bob, Mary, or XYZ Department does." BC/DR professionals can be equally at fault, focusing on what "we need to accomplish," while forgetting that to be truly successful and effective, BC/DR requires enterprise-wide involvement. Even those of us with interrelated responsibilities may tend to develop a standalone approach to our responsibilities. Rather than accept this as "just the way it is," to be truly effective, we need to plan for and take proactive steps to make business continuity and disaster recovery an integral part of the overall organization, its culture, and day-to-day operations. The following section on Evaluating Whether You Have Silos can also be found in the Guidance Appendix.

EVALUATING WHETHER YOU HAVE SILOS

To provide a general indication of how entrenched silo mentality is in your organization . . . in your department . . . at your desk, choose the most accurate response to each of the following ten statements. Be objective as you select the most accurate of three possible responses to each statement:

- True
- Partially true
- Not true

1. Employees have a good understanding of what all other business units do, how they operate, and how they all fit in the big picture.
2. Collaboration is a strong element of the organization's culture.
3. Your peers from other areas of the organization are open to collaborative efforts and joint projects.
4. You believe that silos are detrimental, and you model that belief on an ongoing basis.
5. You encourage your direct reports to collaborate with those outside your business unit.
6. Business units in your organization freely share resources and information with one another.
7. You receive consistent messages from different levels and/or functions within the organization.
8. Your organization has been successful in building commitment for security, business continuity, disaster recovery, and emergency management projects and programs.
9. A vehicle (e.g., work group) exists to facilitate ongoing communication among related functions within your organization (BC/DR/emergency management/security/safety).
10. ALL employees at all levels are aware of the BC, DR, security, and related programs within the organization.

SCORING:
Give yourself:
—10 points for each TRUE response
—5 points for each PARTIALLY TRUE response
—0 points for each NOT TRUE response
Maximum possible points = 100

AVOIDING SILOS

Avoid creating or further strengthening silos. BC, DR, security, and related disciplines demand an ability to solve complex problems that cuts across traditional organizational silos, and in many cases they also require effective integration of multidisciplinary and even multicultural workforces.

Be alert for areas in the organization where business continuity, disaster recovery, and security aren't adequately integrated. Eliminate damaging silo

Score	Assessment
90–100	Outstanding. Congratulations to you and your organization. Continue to avoid silo formation.
70–80	Very good. Look for additional improvement opportunities, and avoid further entrenching existing silos.
50–60	Mediocre. Note which questions were answered "no," and concentrate efforts there.
30–40	Improvement needed. Further assess the situation and develop a plan for positive change.
0–20	HELP!! A great deal of work to be done. Get started now.

thinking whereby you and members of your team focus only on your group's goals to the detriment of other business units and even the organization as a whole. Do everything possible to encourage other business units to be active participants in the BC/DR/security process on an ongoing basis.

Keep the big picture in front of you. Remember that business continuity, disaster recovery, emergency management, safety, and security all have a common mission—to protect the organization and its people, physical assets, and operational capability, and to meet the needs of all stakeholders.

Start by developing and maintaining executive management's commitment. Its support of and involvement in the planning process, training, and testing are invaluable in demonstrating the organization-wide importance of the BC/DR and related programs. Work toward having all functions with a related focus be centrally managed and report to the same executive. For example, consider establishing a department that includes emergency management, security, safety, business continuity, disaster recovery, and risk management and is headed by a person who reports directly to the CEO, CFO, COO, or other position at the upper executive level. The resulting improved communication and coordination will help to ensure that the organization is better prepared to face and recover from disasters.

All employees from the mail room to the boardroom are critical to the overall success of your programs, and each employee has a role to play, be it large or small. Continually educating everyone in the organization about the importance of the BC/DR programs and each employee's roles and responsibilities in carrying out the related strategies and plans is essential. Beginning with new employee orientation, provide the appropriate level of training needed for all employees. Include regularly scheduled reviews and updates.

If you require that business unit managers provide information, develop work-around procedures for their departments, or make employees available to participate in training or a test, ensure they understand why their contribution is important, how it will be used, and where it fits in the big picture. Focus on commonalities, the value to the organization as a whole. Don't stress what's in it for *me* (WIIFM), that it is something *you* need them to do for *your project.* Make certain they are aware of what's in it for *them* (WIIFT)—the value to *their* business units and the organization. Develop partnerships. Make sure there is an understanding that assistance is available if needed, and make the needed help readily available when requested.

If it's not possible to tear down existing silos, build bridges between them by establishing and maintaining working relationships with people in all business units throughout the organization. Get out of your office; avoid being only an e-mail signature or a voice over the telephone. Whenever possible have face-to-face meetings.

Each day when you make your to-do list, be sure to include at least two items that require you to interact with people outside your work group. Avoid the temptation to communicate only via phone and e-mail. Take the time to have lunch or coffee with people both directly and indirectly involved in BC/DR. If there are multiple locations involved in your BC/DR programs, make every effort periodically to visit those locations. Offer help by sharing resources with other departments, including information, equipment, and time. Introduce yourself and the organization's BC/DR programs to new department managers. Be available to acquaint them with the BC/DR programs, and bring them up to speed on their business units' involvement.

Beware of using jargon and terminology that is unique to your area of responsibility. As an example, if you're involved in business continuity planning, avoid communicating in "business continuity-ese" when interacting with those who are not directly involved in business continuity planning. Avoid using our favorite acronyms—such as BCP, DRP, BIA, RTO, and RPO. It is likely that these are not much more meaningful to most people than a bowl of alphabet soup and can lead to those not directly involved in business continuity planning feeling like "outsiders" being excluded from an exclusive club. In addition, make sure a common vocabulary of terms in used universally throughout your organization.

Establish a BC/DR planning group composed of representatives of all major business units. This representation gets people from multiple areas of the organization involved and invested in the process and enhances BC/DR visibility. Beyond BC/DR benefits, representation from multiple areas assists in building better understanding of how other departments function and a greater awareness of the interdependencies between business units. To the extent possible, the planning team should be composed of those who will be carrying out the developed strategies and plans when a disaster occurs. This leads to plans that are considered the property of the end users (*our plans*), rather than plans that belong to those with primary responsibility for BC/DR planning (*your plans*).

Be open to suggestions. Ask for and truly listen to feedback. Remember that BC/DR is still relatively uncharted territory and that none of us knows everything or the best way to do anything. Realize that we don't yet have all the answers. Those not directly involved in BC/DR who are looking at strategies and procedures with a fresh set of eyes may have ideas for new approaches that are of tremendous value. This openness and the involvement of others in the planning process help make our programs and plans better and something that belongs to the entire organization, not just those directly involved in BC/DR.

In today's complex world that constantly delivers new challenges for those charged with keeping organizations operational in the face of disasters, there can no longer be independent silos. One silo cannot successfully manage risks. If we cannot tear down the silos, we must make sure that all efforts related to disaster management are interdependent and coordinated.

Develop a working network among those with similar and interrelated responsibilities, for example, safety coordinator, security director, disaster recovery manager, business continuity coordinator. Representatives from human resources, facilities, or engineering might also be included if they have responsibilities related to responding to emergencies and disasters. Take it upon yourself to establish and foster effective lines of communication and working relationships with these important partners. Go out of your way to say hello and touch base with these allies at times when you are not asking them for something.

Once established, maintain your relationships with others through mutual trust and respect. Walk your talk. Mistrust and disrespect allow silos to flourish.

Another subgroup of silos that can form is the various business continuity–related functions including emergency preparedness and response, business continuity, disaster recovery, security, safety, and so on.

To help avoid polarization among these functions, consider forming a peer group that includes all BC/DR-related functions. The key here is that it be a true "peer" group. When bosses are in the room, the consequence may be a reduced comfort level, with more vulnerability and more motivation to look good rather than openly and honestly collaborate and share information.

Focus on individual or shared work issues and challenges. These peers may have some excellent suggestions for a project you're tackling, and you may discover some opportunities to work together on projects. When the issues are compelling and the work results in tangible benefits on the job, the benefits of meeting as a group become even more evident.

Commit to meeting on an ongoing, regular basis to help ensure that group discussions translate into action. It takes time to overcome the effects of a silo history. After several meetings, relationship and trust are strengthened. Continuing to meet over time results in moving beyond the exchange of surface-level information and office gossip to addressing deeper challenges and mutual problem solving.

Collaboration with these fellow employees will result in not only a safer and more secure working environment for everyone but also a greater organizational capability to continue or more rapidly resume operations following a major emergency or disaster. A synergy of functions including security, business continuity, contingency planning, and disaster recovery, and—as appropriate based on roles and responsibilities—human resources, safety and health, purchasing, facilities management and real estate, and other key areas creates programs that are better integrated into the organization's culture and operations and, therefore, much more effective.

Never assume that help, assistance, and cooperation are not available or that employees from other departments are not interested in what you are doing. Ask for involvement. Don't wait until after a training, test, or other activity only to hear a department manager or other colleague say, "If I had known you needed help, I would have volunteered," or "I would have welcomed a chance to be involved in or to learn more about. . . ."

Articles in organization newsletters and on an intranet and announcements at departmental and other work group meetings can help familiarize all employees with BC/DR. Use break room and cafeteria bulletin boards to promote your programs. Be available to speak at internal meetings and training sessions.

Don't forget the basics. Even when time is at a premium and a project task deadline is looming, *make* the time to recognize and thank those who have made a contribution. Send an e-mail to a BIA survey respondent; make a phone call to the person who developed a business unit's continuity plan; or pay a visit to a department manager who made employees available to participate in a hot site test. These seemingly simple, yet often overlooked, steps both provide appropriate recognition and build the working relationships that help tear down silo walls.

CONCLUSION

Continually look for ways to prevent silos from being built, to establish and maintain bridges between existing silos, and to avoid the damage that can be caused by silos. Although this takes time and effort, this time is well spent and will lead to programs that involve and benefit the entire organization, rather than becoming another silo.

See also Managing Organizational Culture and Change Acceptance.

WINNING ACCEPTANCE FOR SECURITY OR OTHER NEW PROGRAMS

W. Timothy Coombs

It seems reasonable that an organization would embrace ideas such as information security and business continuity. There is clear evidence that both benefit an organization. The problem is that organizations are just a collection of people. People regularly do things that are bad for them, such as driving over the speed limit and eating fatty foods. Like the people who populate them, companies can be irrational and avoid doing things that are good for them. This means it is naÏve to assume people will just embrace and support efforts to introduce a new program. The key to winning acceptance of a new program is to anticipate resistance and devise a strategy for overcoming it. Here are some tips for winning acceptance of new programs that can be applied to security and business continuity.

STARTING POINT

The starting point is to develop your arguments for a new program—your central message. Begin by outlining why the program is needed and how such a program will benefit the organization. These are your basic talking points. Presenting bulleted lists can be boring, so you need a good story. Craft a vision around the new program. A vision is story—a picture of what the organization will be like with the new program. Paint a picture of how the new program will assist an organization in surviving common business problems faced in your industry. You are helping people to visualize the new program, and visualization is a powerful persuasive tool. Have a short and a long version of your message, because sometimes you have a minute or two to make an informal pitch and other times ten to fifteen minutes for a formal presentation. All of your later messages designed to win support will come from this central message.

Your early efforts will concentrate on developing a core group of supporters for the introduction of the new program. The first step is to identify the people in management who make the real decisions. This typically includes top managers. Without their support, you stand no chance of introducing an effective new program. The second step is to consult with employees who will be involved with the new program once it begins. These people must become a part of the process from the start. Ask these employees for their input on the project, thoroughly brief them on why a new program is being developed, and update them on the progress of the project. You need to secure buy-in from this core group.

RESISTANCE TO CHANGE

Now you are ready to tackle the organization as a whole. Keep in mind that introducing a new program is a form of organizational change, and in general, people do not like and will resist change. Organizational change creates anxiety because it is new and unknown, and inconvenient, as people must alter their schedules and learn new things. Be prepared for resistance. Negative reactions to change follow a pattern of denial, anger, bargaining, and acceptance. Develop message strategies that can counter any and all of these four negative reactions.

Denial should not be dismissed. Instead, acknowledge people's concerns about the new program. Review the positive and negative aspects of the change. Do not just push the positive parts, or you will sound like a used car salesperson. But return to your central message and reinforce why a new program will be worth the effort. Anger is unpleasant, but do not take it personally and do not escalate the anger with a like response. Let people vent their feelings. Most people will feel better after they complain, and it shows you respect their feelings. You need thick skin to deal with angry employees.

Bargaining means you can be flexible on inconsequential matters. For instance, you can negotiate the exact date the plan takes effect, the colors of the binders, and the name of the plan. However, you must hold firm on the basic position that a new program will be part of the organization's future. Think about which points can and cannot be changed. Knowing this in advance makes the bargaining phase go more smoothly. Once people accept the business continuity program, praise them for their support. Resist the temptation to gloat or ridicule their reluctance. Praise will help ensure that the business continuity program functions smoothly.

CHANNELS AND VIVID EXAMPLES

There are two final points to think about once you have developed your central message and prepared to address the various negative reactions to change: the communication channels and vivid examples. The communication channels you use are a critical decision. Common communication channels used by managers include meetings, e-mails, memos, and reports. It is important to use a mix of channels to reinforce your message. Also, the various channels differ in terms of being dynamic. Dynamic channels allow the receiver of the message to give feedback to the sender. Feedback will help you, the sender, understand what type of negative reaction you are encountering. The most dynamic channels involve face-to-face communication such as meetings. Make sure meetings are used in the mix of communication channels to provide employees a chance to give feedback and to ask questions. They also give you a chance to assess the types of negative reactions and the level of resistance.

Finally, develop some vivid examples to illustrate key points. Statistics are important and will be the base for many of your messages. A cost-benefit analysis or statistics about the number and types of business disruptions in your industry are critical to have. However, anyone who has sat through a budget presentation knows that statistics alone can be boring and easy to forget. Vivid examples, using colorful words and details, are needed to illustrate your statistics and facts and make the information more engaging and easier to remember. Consider the following example. Your data show the number of IT-related business problems in your industry and the total cost of those disruptions. Now, take one specific case and give the details. How and why did the disruptions occur? How much money did the company lose and why? How were the employees affected by the problem (lost wages, benefits, and/or stock price)? The details make the statistics real for people—they bring the data to life. Vividness connects back to the vision you created for the central message. The vision of a future with the new program should be vibrant. It can even include an alternate view of the future should the organization not adopt the new program.

CONCLUSION

Introducing a new program into an organization can be difficult. If you are fortunate, people will love the idea and embrace your change. But, it is important to prepare for the worst-case scenario. Create your central message complete with talking points and vision. Get your core group of supporters to buy into the business continuity program. Be prepared to respond to any and all of the four negative reactions to change. Finally, be sure the communication channel mix includes some face-to-face interchange, and use vivid examples to support your statistics. The better prepared you are for resistance, the greater the likelihood your organization will adopt a functional business continuity program.

See also Managing Organizational Culture and Change Acceptance.

MANAGING ORGANIZATIONAL CULTURE AND CHANGE ACCEPTANCE

W. Timothy Coombs

A recurring theme in many of the topics related to business security is the need for winning acceptance of changes. This can include the development of business continuity programs, use of computer security protocols, or acceptance of ethics and compliance codes. New policies and programs are a form of organizational change. One thing we do know is that change is never easy in an organization. This entry examines the role of organizational culture in managing change.

People naturally resist change because it creates something new and different. People in an organization have to learn new behaviors with a change, which requires investing their time. There is also the possibility that people will not be successful in learning the new behaviors. Any or all of these factors can lead people to resist change efforts in an organization.

WHAT IS ORGANIZATIONAL CULTURE?

In general, organizational culture is the way things are done in an organization. Organizational culture represents the beliefs, values, norms, and practices that are taken for granted in an organization and guide actions in the organization. Some people make the mistake of assuming the culture is the same as the mission statement or vision statement. That may not be the case if people in the organization do not live by the mission or vision. The organizational culture is a manifestation of what is important in the organization and what directs people's actions and thinking. Cultures evolve over time and are difficult to control.

ASSESSING ORGANIZATIONAL CULTURE

Before trying to change a culture, management needs to know what the culture is. A variety of methods can be used to assess the current culture, including surveys, focus groups, interviews, observations, and an analysis of organizational documents such as web sites, policies, newsletters, and manuals. Utilizing these research tools enables understanding of what is important in the organization—its core values. Focus on what employees believe management pays attention to, what actions are rewarded or punished, and what beliefs and values seem to dominate messages in the organization. Because we have a hard time seeing our own culture, it may be helpful to bring in a consultant to facilitate assessing the organization's culture.

SKEPTICISM IN THE ORGANIZATIONAL CULTURE

An analysis of the organizational culture can determine whether there is skepticism in your organization about change. Skepticism is when employees doubt a change will succeed. This intensifies employee resistance to change because they see the effort as a waste of time. Experts in change management refer to this phenomenon as organizational cynicism. A culture plagued by organizational cynicism reflects a lack of faith in the leadership to make successful changes. Typically, organizational cynicism is a result of past change failures. Employees are pessimistic that any change will work and blame management for past failures. Organizational cynicism is reflected in comments such as the following:

- "Most of the programs that are supposed to solve problems around here will not do much good."
- "Attempts to make things better will not produce good results."
- "Suggestions on how to solve problems will not produce much real change."
- "Plans for future improvements will not amount to much."
- "The people responsible for solving problems around here do not try hard enough to solve them."
- "The people responsible for making things better do not care enough about their jobs."
- "The people responsible for making improvements do not know enough about what they are doing."
- "The people responsible for making changes do not have the skills needed to do their jobs."
- "The people responsible for solving problems around here cannot really be blamed if things do not improve."
- "The people responsible for solving problems around here are overloaded with too many job responsibilities."

- "The people responsible for fixing problems around here do not have the resources they need to get the job done."
- "The people responsible for making changes around here do not get the cooperation they need from others."

Organizational cynicism can be overcome through strategic change efforts. Management must be willing to confront the past failures that have bred the organizational cynicism. Management must acknowledge and explain past failures, which includes owning up to its own contributions to those failures. Be sure to talk about past success as well so that employees remember change can work.

STRATEGIC APPROACH TO CULTURE MANAGEMENT

Change needs to be planned carefully. Management must be strategic in its approach to change management if it wants the change to take root and flourish. There are six steps in the strategic approach to culture management: (1) change evaluation, (2) cadre construction, (3) message development, (4) organizational buzz, (5) cultural reification, and (6) progress monitoring.

Change evaluation seeks to decide whether the change is consistent with the existing culture. Management must determine whether the change is like something the organization already does or values. Management needs to find a connection to current culture because this connection makes the change less threatening. Management must also determine what new "features" need to exist in the culture to support the change. It will also need to develop a framework to support the desired change.

Cadre construction organizes a group of people who support the change. This serves as a foundation for change acceptance. The cadre construction should include what management researchers call prime movers—powerful figures in the organization that others look to for guidance or rely on as important sources of information. Involving a wide number of people in the cadre helps to create greater buy-in to the change.

Message development involves creating a vision for the change and talking points for the change cadre. The vision indicates what the future of the organization can be when the change is in place. It is a picture of what the organization can become. The vision creates a sense of purpose but must be realistic. Management should avoid overpromising and setting up the change for failure. A talking point is a short rationale for the change. Talking points can include current vulnerabilities, the problems with the status quo, and how the organization will benefit from the change. The talking points also need to create a sense of urgency.

Organizational buzz attempts to get people in the organization talking about the change. This is a time when past change failures must be addressed. Management must send messages about the change through multiple communication channels, including an intranet, newsletters, e-mails, position papers, and town hall meetings. Management must also solicit feedback from people in the organization. In this way management answers questions people might have about the change.

Cultural reification happens when management integrates the change into the day-to-day operations of the organization. The policies and behaviors become linked to employee evaluations. Some organizational rewards or punishment will be tied to the change. Finally, management must monitor the change to determine whether it is successfully taking effect. Are new policies being followed? Are new appraisal items being used? Are rewards and/or punishments being delivered consistently? If the change is failing, the change management effort should be adjusted.

CONCLUSION

As organizations look to implement or to improve policies related to business security, management will have to grapple with organizational change. Culture is an essential factor in getting change to become an effective part of the organization. People must become comfortable when change is introduced into an organization. Because change can create uncertainty, stress, and resistance, communication is essential to helping people accept a change and its becoming integrated in the organizational culture. A carefully constructed plan is needed to help an organization manage its change.

See also Crisis Management; Avoiding the Silo Effect to Improve Business Security. and Winning Acceptance for Security and Other New Programs.

CULTURE OF INTEGRITY

W. Timothy Coombs

Millie Kresevich, a retail loss-prevention specialist, believes one mechanism for reducing misconduct in organizations, including employee theft and fraud, is to develop a culture of integrity. Employees must learn to talk about integrity, comply with ethics policies, and deal with problem situations.[1] A culture of integrity is something that management must craft. The following four principles serve as a foundation for a culture of integrity:

1. Have a clear statement of the organization's ethical policies, and explain them to every employee.
2. Model ethical behavior for all employees.

3. Encourage everyone in the organization to talk about ethics.
4. Make adhering to the policy on ethics part of employee evaluation. Ethical behavior must be rewarded, and unethical behavior punished.

As noted in other entries related to ethics, management conduct is critical to an effective ethics program. Employees will follow the examples set by management. Managers can lead by example with integrity. Management must learn to trust others, become a good listener, clarify expectations about integrity, and help to create a climate of honesty.

Kresevich has developed a training program designed to facilitate a culture of integrity. The program teaches employees communication skills, how to comply with ethics policies, and how to address specific ethical situations. The training centers on a twenty-four-page workbook containing ethics exercises. It places employees in ethical dilemmas so they can work through the problems with other employees. The exercises emphasize the issues that helped to create the situation rather then just the behavior or feelings. A series of questions guides employees through the scenarios, which provide insights beyond the specific problems. Trainees learn why people do not commit to ethical policies and how to react to unfair situations. One sample scenario involves a top-producing employee coming in late regularly. Participants are asked the following questions: "What would you do and why?" "What would you say to the employee that was late?" "What is the benefit of addressing the situation?" and "What is the impact if you do not address this?" The questions allow trainees to dig deeper into the issues and gain richer insights.[2]

CONCLUSION

Training in integrity can help to reduce theft, improve morale, and increase profitability. Although we want to believe employees naturally bring integrity to the workplace, this is not always the case. Employees simply might not know what is an ethical violation and how they should behave in situations that could compromise ethics. Having a clear policy and training employees according to that policy help to reduce uncertainty about ethics and promote an ethical workplace. Organizations can benefit from ethical policies and training employees about those policies and the idea of integrity in general.

See also Corruption as a Business Security Concern; Ethics as a Business Security Concern; and Ethical Conduct Audit.

NOTES

1. Millie Kresevich, "Using Culture to Cure Theft," *Security Management*, Feb. 2007, pp. 47–51.

2. Kresevich, "Using Culture to Cure Theft," pp. 49–51.

EXERCISE AND TRAINING BASICS

W. Timothy Coombs

Every response plan developed by an organization should be practiced and tested. This includes emergency management plans, business continuity plans, and crisis management plans. Plans are practiced and tested through exercises. People practice putting the plans into action and the plans are examined for any weaknesses. An exercise is a focused activity that puts organizational personnel in a simulated situation requiring them to act as they are expected to in a real event. Exercises involving emergency plans will be used for illustrative purposes in this entry, but the concepts and ideas can be applied to any type of response plan.

WHY EXERCISE?

A plan is an idea that should work. An actual event is not the time to discover the plan does not work or that individuals charged with enacting the plan cannot do so. The two main reasons for exercises are (1) for individual training as people experience their roles and (2) for system improvement as plans and personnel are adjusted. Exercises test and evaluate the plans, policies, and procedures. The organization finds out whether the plan can work. A weakness in the plan or lack of resources is revealed in a low-risk environment. Exercises clarify roles and responsibilities, help personnel improve their individual performances, and develop coordination and communication between units and people in the organization.

Exercises are used to spot and correct problems before an actual event. The end result should be a more complete plan and a more effective response to an event. Some organizations are required by regulations and laws to engage in exercises. Airports, health care facilities, and nuclear power plants are obligated to hold regular exercises. The Occupational Safety and Health Administration (OSHA) requires employers to develop emergency plans. Organizations in which chemicals are produced, used, or stored are to conduct yearly exercises and evaluate their hazardous materials response and recovery plans.

PROGRESSIVE EXERCISING

An exercise program uses a variety of types of exercises. The idea is for an organization to perform a series of different types of exercises that build in complexity. Each exercise is designed to achieve particular goals and builds upon the results of the previous exercise. An exercise program demands careful planning and specific goals. The progression in complexity is designed to build confidence. People are able to master a set of skills before more demands are placed on them. The people involved in an exercise vary by the nature and size of the exercise. The progression also serves to increase the number of people involved in the exercise. By the final stage, your organization will be coordinating with local emergency responders as part of the exercise.

An exercise program cannot be developed overnight. Management must examine capabilities, costs, scheduling of tasks, and developing a long-term plan. A planning team should be developed with representatives from across the organization and perhaps even some community responders. The team can develop a plan and adjust that plan, as early exercises indicate how well the organization is or is not progressing.[1] The Exercise Program Rationale table reviews the reasons to conduct an exercise program.

Exercise Program Rationale

Reasons to Conduct Exercise Program Activities[2]				
Orientation	Drill	Tabletop Exercise	Functional Exercise	Full-Scale Exercise
No previous exercise	Assess equipment capabilities	Practice group problem solving	Evaluate a function	Assess and improve information analysis
New plan	Test response time	Promote management familiarity with plans	Observe physical facility use	Assess and improve cooperation
New procedures	Personnel training	Assess plan coverage for a specific situation	Reinforce established policies and procedures	Test resource and personnel allocation
New staff or leadership	Verify resource and staffing capabilities	Assess plan coverage for a specific risk	Test seldom-used resources	Assess personnel and equipment locations
New industrial risk		Examine staffing contingencies		
		Test group message interpretation		
		Observe information sharing		

EXERCISE TYPES

A comprehensive exercise program is composed of five types of exercises: (1) orientation session, (2) drill, (3) tabletop exercise, (4) functional exercise, and (5) full-scale exercise. The Exercise Comparison table summarizes the value of each type of exercise.

Orientation Session

An orientation session introduces the plan and process. The purpose is to familiarize people with their roles, plans, procedures, and equipment. It can also help them understand how to coordinate activities and clarify their responsibilities. There are no set rules for conducting an orientation session. The facilitator must carefully plan the orientation session and keep it moving. This is not a time to make it up as you go along or to let people drift off on tangents. Be creative and try to involve the participants in the process. There should be interactivity in the session to keep people connected to the discussion.

Key characteristics:

- *Format*. It is a low-stress exercise that is usually presented in a group setting with rather informal but structured discussion. A variety of formats can be used including lecture, discussion, slide or video presentation, computer demonstration of software program, panel discussion, and guest lectures.
- *Applications*. The orientation session can address a number of purposes, including the group discussion of a problem or topic; introduce new ideas or concepts; inform new people about existing plans and procedures; discuss the progressive nature of exercises; or motivate participants to be involved in future exercises.
- *Leadership*. Orientation sessions are guided by a facilitator, who should organize the session, present the information, and guide the discussion.
- *Participants*. The participants are cross-functional, drawn from a variety of departments in an organization.
- *Facilities*. Orientation sessions can be conducted in conference rooms or training rooms. The location depends on the size and equipment needs of the session.
- *Time*. Orientation sessions should last from one to two hours.
- *Preparation*. Preparation time is fairly short, usually about two weeks. Participants are not required to have had previous training.

Drill

A drill is a supervised, coordinated activity used to test a specific operation of part of a response plan. The idea is to work on smaller parts of the response plan before integrating these components into a large drill that tests them all.

Exercise Comparison

Comparing Five Types of Exercises[3]

	Orientation	Drill	Tabletop Exercise	Functional Exercise	Full-Scale Exercise
Format	Informal discussion in group setting Variety of ways to present it	Actual facility response Actual equipment	Narrative presentation Problem statement and simulated messages Group discussion No time pressure	Interactive Players respond to messages given by simulators Realistic but equipment is not used Real time and stressful	Realistic event announcement People gather at assigned locations Actions on the scene are the input for the participants
Leaders	Facilitator	Manager or exercise designer	Facilitator	Controller	Controller(s) Evaluators
Participants	Cross-functional	People involved with the function being tested	Anyone who may be involved with the particular event	Players Simulators Evaluators	All people who might be involved in the event
Facilities	Conference or training room	Command center and the field	Conference or training room	Command center and other rooms	The entire facility
Time	1 to 2 hours	1/2 to 2 hours	1 to 4 hours	3 to 8 hours	1 hour to 2 days
Preparation	2 weeks	1 month	1 month	At least 6 months	About 1 year

An example would be an evacuation drill or a test of the organization's emergency notification system. Begin a drill by briefing participants on the scenario to be used and the function of the drill. Prepare for the drill by carefully reviewing the part of the response plan to be tested. During a drill, monitor its progression, making sure participants are taking the expected actions. If they are not, the drill designer needs to provide messages to prompt those actions. The drill tests specific tasks and skills, so you must make sure the participants engage in those tasks and use those skills.

Key characteristics:

- *Format*. Drills involve actual field responses. They should be as realistic as possible and use any equipment that would be needed during an actual event.
- *Applications*. Drills work on specific tasks and skills. They also provide training on new equipment, new policies or procedures, and maintenance of current skills. For instance, a chemical facility might work on evacuations, isolating a spill area, or valve system shutdowns.
- *Leadership*. The person in charge could be a manager or an exercise designer who must have a thorough understanding of the tasks and skills being tested.
- *Participants*. The people involved are those associated with the specific task or skill being tested.
- *Facilities*. Drills are conducted on-site where the task or skill would need to be performed.
- *Time*. Drills run from a half hour to two hours.
- *Preparation*. Drills are fairly easy to design. Preparation time is usually a month. Part of the preparation includes creating a short orientation for the drill.

Tabletop Exercise

Tabletop exercises are designed to be low-stress analyses of problematic situations an organization is likely to face. The tabletop, led by a facilitator, is not an attempt to simulate the event or use equipment, but is just an analysis of the situation. Participants improve their critical thinking skills by analyzing and resolving problems using plans and procedures. The key is to have participants identify and analyze the problem areas.

Key characteristics:

- *Format*. A tabletop begins with people reading a short narrative about the event. The facilitator then starts the discussion with a problem statement describing major events. Participants then talk about how they might respond. The facilitator also uses simulated messages to further the discussion. These messages are more detailed than the problem statement and add

more information to the discussions. The simulated messages mirror how teams learn more about an event as it unfolds. The discussion should focus on roles (how a person would respond), plans, coordination between units, the effects of decisions, and similar concerns.
- *Applications*. Tabletop applications include the following: low-stress discussions of plans and procedures, favorable conditions for problem solving, allowing team members to get to know one another better, and serving as preparation for a functional exercise.
- *Leadership*. The facilitator who leads the tabletop decides who gets messages, calls on particular people for comments, asks questions, and tries to keep the decision making on course.
- *Participants*. The organization should select participants who would be involved in that particular event so that they can practice their roles.
- *Facilities*. A large conference room or training room is used depending on the number of participants and the equipment requirements.
- *Time*. Tabletops generally run from one to four hours but can be longer. The facilitator wants to give people a chance to discuss topics fully, so there are no time pressures. The aim is not to get through all the material but to have arrived at decisions based on in-depth analysis.
- *Preparation*. Tabletops take about a month to prepare. Participants should have been through an orientation session and one or more drills prior to a tabletop.

Functional Exercise

The functional exercise tests the capabilities of the organization to respond to a simulated event. As a simulation, it is interactive and time pressured. Events and information unfold in real time. The functional exercise allows an organization to examine the coordination, interaction, and integration of its roles, policies, procedures, and responsibilities.

Key characteristics:

- *Format*. Functional exercises are interactive. They simulate events but do not involve moving resources or using equipment. Simulators provide messages to participants in a carefully planned sequence that mimics the actual event. These messages make information available and present problems that participants would encounter in the actual event. The idea is to see how well the participants or “players” can coordinate and use the plans and procedures to address the event. The exercise is high stress because it requires real-time decisions and actions. Players experience the consequences of their actions, and their decisions and actions influence the development of the exercise. Creating the specific messages and anticipating contingencies make a functional exercise difficult to construct.

- *Applications*. Specific response functions—actions or operations required during a response—are tested. Examples would be damage assessment and coordination of units. Testing functions is the last step before a full-scale exercise.
- *Leadership*. Functional exercises require a controller who manages and directs the exercises.
- *Participants*. Include players, simulators, and evaluators. Players are the organizational personnel who would be involved in the particular function in that specific situation. The simulators play external roles, such as the fire chief, and deliver the planned messages to the players. Evaluators only observe and assess performance. They do not interact with players.
- *Facilities*. The organization's command center is a designated area to be used in emergencies or crises. Players should gather where they would be during the event.
- *Time*. It takes three to eight hours for a functional exercise.
- *Preparation*. It takes organizations six to eighteen months to plan a functional exercise. Due to the complex nature and time consumption, organizations may consider hiring a vendor that specializes in running simulations. The vendor can customize the exercise to your organization's needs and supply the materials, controller, simulators, and evaluators. An additional benefit of vendors is the third-party evaluation of performance. Their critiques are not influenced by workplace relationships.

Full-Scale Exercise

A full-scale exercise simulates an actual event as closely as possible. Equipment is used, people mobilized, and simulated victims appear. The organization often coordinates the full-scale exercise with local emergency responders. These responders get practice, and the organization better understands how to coordinate responses with these units. Your people are on the scene moving and using equipment as they would in the actual event, as well as coping with the simulated victims. This is the most stressful of the exercises and is executed in real time.

Key characteristics:

- *Format*. People are given a description of the event just as they would be in a real event. This might mean telephone calls or a warning siren. Those who must go to the field take their places and cope with the simulated problems encountered there. The command center should be operational and directing the response. Those assigned to the command center take their places to engage in their roles.
- *Applications*. Full-scale exercises are the ultimate test to reveal whether people can do what they should during an event and how well the plans and procedures work in an event. The downside is the cost and time commitment.

- *Leadership*. There will be one or more controllers and multiple evaluators. The controllers will send the necessary messages to participants.
- *Participants*. Anyone who might be involved in the actual event is included. Evaluators are needed too.
- *Facilities*. The event unfolds across the organization's facility and must include the command center.
- *Time*. Full-scale exercises can be as short as two to four hours or last one or two days. It depends on the scope and nature of the event.
- *Preparation*. It can take a year to prepare a full-scale exercise. As with functional exercises, organizations should consider hiring a vendor to develop and run the full-scale exercise.

The exercise process encompasses a variety of tasks. FEMA organizes exercise tasks in a two-by-three matrix involving the exercise phases (preexercise, exercise, and postexercise) and the type of task (design or evaluation). The Task Categories table reviews the range of tasks involved with exercises.[4]

THE EXERCISE PROCESS

It is best to think of exercises as a process rather than an event. The exercise process is composed of five accomplishments: (1) establishing the base, (2) exercise design, (3) exercise conduct, (4) exercise critique and evaluation, and (5) exercise follow-up.

Establishing the Base

The purpose of any exercise is to get people to think or act the way they would in a real situation. Management begins by laying a foundation—known as establishing

Task Categories

	Preexercise Phase	Exercise Phase	Postexercise Phase[5]
Design	Review plan Assess capability Determine cost and liabilities Organize design teams Build support for an exercise Draft a schedule Design the exercise	Prepare facility Assemble props Brief participants Conduct exercise	
Evaluation	Select evaluation team Develop evaluation methodology Select and organize evaluation team Train evaluators Contract the evaluation	Observe assigned objectives Document actions	Assess achievements of objectives Participate in postexercise meetings Prepare postexercise report Participate in follow-up activities

the base—for the exercise to be sure it gets the desired results. To prepare for an exercise, management must review the current plans, assess the organization's ability to conduct a drill, define the scope of the exercise (its limits), select the type of exercise based upon organizational needs, consider the costs and liabilities, develop a statement of purpose, and build interest and support for the exercise. Three of these points require elaboration here.

Current plans outline responsibilities for personnel during an event and include contact information. They are also a reference tool for decision making and problem solving. The review of a plan should consider the types of situations (hazards and risks) covered; the roles people are to play in various situations; current training level of team members; and a review of the personnel, resources, and procedures outlined in the plan. You are looking for areas that could use improvement or revision.

Management must determine whether the organization is ready for a particular exercise. Reviewing the last exercise helps establish what the team would be ready for next. Is it prepared to advance to the next level, or is there a need to work on existing skills? Does the desired exercise fit into the upcoming schedule of the personnel who need to be in the exercise? Why have an exercise if the participants will not have time to spare to be fully involved. Costs and liabilities are a related issue. Does the organization have the financial resources to cover the desired exercise? Exercises have costs including employee salaries, equipment, materials, and there are vendor fees, if an exercise is outsourced. An organization must also review its insurance to ensure coverage for possible injuries or equipment damage during an exercise.

Exercise Design

Exercise design is one of the most complicated stages. The design team must create the materials necessary to have an exercise. This exercise design process covers eight points: assess needs, define scope, purpose statement, objectives, narrative, major and detailed events, expected actions, and exercise messages. Needs assessment helps the design team in selecting an appropriate scenario for the exercise, one that fits with the hazards or risks an organization is most likely to encounter along with the actions and skills it has identified as needing to be addressed. A key part of needs assessment is the results of the last exercise. What still needs work, and which areas of the response are ready for more intensive testing?

The scope sets limits to the exercise. One exercise cannot test everything. The scope narrows the focus of the exercise and flows from the needs assessment. It should consider the type of event, the participants involved in that event, the location of the event, and the functions to be tested in the event. The scope is also shaped by the available budget and personnel.

The purpose statement—a broad articulation of the exercise goal—guides the entire exercise. The purpose statement limits the objectives and clarifies to participants why the exercise is being conducted. Objectives are more specific and describe the performance you expect from the participants. Objectives are critical to the entire design process. The exercise events need to capture the objectives, whereas the evaluation is based on the performance of the behaviors specified in the objective. Good objectives are concise and clear. An objective is written with an action phrased in observable terms, the conditions under which the action is to be performed, and the standards of performance. The objective states who should do what under what conditions according to what standards. A sample objective can found in the Objective and Expected Action box. FEMA recommends the SMART guidelines for objectives. An objective should be *s*imple, *m*easurable, *a*chievable, *r*ealistic, and *t*ask oriented.

The narrative briefly describes the events that occurred right before the exercise began. The narrative sets the mood for the exercise as well as the stage

Objective and Expected Action: FEMA Example for Airplane Crash

Function: Coordination and communication between the airport and the emergency responders.

Objective: Upon notification that a crash is imminent, responding unit will stage within three minutes according to the emergency plan.

Event: Landing of disabled aircraft is imminent.

Expected Actions: Airport
Notify police, fire, and medical personnel.
Alert hospitals to potential mass-casualty incident.
Activate its response team.

Hospital
Notify other medical facilities as appropriate.

Crash/Fire Rescue
Initiate command center.
Notify dispatch of command center and staging areas.

Possible Messages: Radio call from plant to tower.
Tower calls police, fire, and rescue.
Plane requests runway to be designated.
Call from hospital requesting information.
Calls to dispatch from media.
Degrading radio communications with plane.
Pilot feels major vibrations/noise on the plane.[6]

for later actions by providing the initial information players use to make choices and take actions. It is akin to the briefing people receive when an actual event begins. A good narrative is about five paragraphs long, is very specific, is phrased in the present tense, presents a chronology of events, is written in short sentences, and emphasizes the critical nature of the event. Points to consider for a narrative include what the event is, the danger surrounding the event, how the organization learned of the event, reported damage, sequence of events, where the event is, the weather conditions, and whether there was any advanced warning. The Sample Narrative box provides a sample exercise narrative from FEMA.

Major and detailed events serve to organize the development of the scenario. These are large or small events or occurrences that are created by the major event presented in the narrative. Major and detailed events supply a structure that links the simulated events to the actions people need to take and provide unity to the exercise as it unfolds. Major events are the big problems resulting from the event. Detailed events are specific problem situations that require a response from participants. Detailed events should prompt one or more expected actions from the players. The design team picks events that fit with the objectives and the actions it wants the players to take.

Here are sample major and detailed events FEMA provides for an airplane crash.

Sample Narrative

Here is a sample exercise narrative from FEMA:

A Boeing 747, en route from Panama to San Francisco, is experiencing in-flight engine problems and will have to make an emergency landing. Plans have been made to land at a large airport 200 miles north. However, the latest communication with the pilot indicates that the plane has lost engine power and is losing attitude too quickly to reach the large airport. Even though your city airport is too small to handle a 746, you are the only hope for the 350 passengers and 10 crew members.

Conditions at your airport are clear and the surrounding area is dry. A hot, dry wind is blowing from the north.

The main runway lies along a relatively unpopulated suburban area. However, the likelihood of the pilots being able to control the huge plane and stay within the landing space is slim. The approach passes over populated suburban housing developments. The airport control tower alerts its own crash/fire rescue units and requests that the local emergency services provide backup assistance in fire, police, medical, welfare, and search and rescue capabilities.[7]

> *Major events:* Fuselage breaks apart and hits buildings on the ground, several homes in the area are ignited by jet fuel, survivors are believed trapped in the front section, a crowd gathers near the crash including family members of victims, bystanders are injured on the ground, and casualties are estimated at between 100 and 150.
>
> *Detailed events:* Mortuary capacity is too small to accept the large number of remains, local hospitals do not have the specialized burn care needed by victims, and the American Red Cross has agreed to fund a family information center.

The expected actions are the actions or choices that you want players to carry out in order to demonstrate their competence. In short, it is what you want people to do so you can evaluate their proficiency. The expected actions shape the messages developed for the exercise. The messages must lead people in the direction of the desired actions. The expected actions are drawn from the performance expectations of the objective. The desired actions are essential to evaluation because they tell evaluators what to assess. There are four basic actions: verification, gather and verify information; considerations, consider information and discuss among players; deferral, defer action to later; and decision, deploy or deny resources. The Objective and Expected Action box contains sample actions.

Finally, the design team prepares the messages used to communicate details of unfolding events to the players. The messages that relate the major and detailed events to the participants can be delivered by telephone, e-mail, radio, fax, written notes, or in person. The messages should have a direct connection to expected actions. The Objective and Expected Action box also contains some sample messages. Each message must have the source (who sends the message), the transmission (how the message is sent), message content (what is in the message), and recipient (who is to receive the message). The Message Format box illustrates how FEMA recommends creating messages. Not surprisingly, exercises do not always go as planned, as players respond differently than anticipated. Spontaneous messages, used to address the off-script developments, need to be created quickly but with care. Controllers and simulators must remember the four message factors and try to keep the messages realistic and consistent with the exercise scenario.

In the end, a design team's master scenario of events is used to monitor the development of the exercise and help keep it on track. The information can be converted into a chart that provides guidance for the controllers and simulators.

Exercise Conduct

Exercise conduct involves the leaders and participants taking part in the exercise. A successful exercise depends on a number of factors. Participants must have a clear understanding of the rules for the exercise and what is expected from them. Controllers and simulators must provide a consistent flow of messages. The messages serve to sustain action by providing participants with something to react to. Participants must be encouraged to take the exercise

Message Format

This is the format FEMA recommends for preparing exercise messages.[8]

Emergency Exercise Message

To: Method: From:

Number: Time:

Content:

Actions Taken:

seriously and treat it as a real event, not as a mere game. They need to know there will be consequences if they do not take the exercise seriously. To aid the realism, a valid timeline for an event is required. If the exercise does not mirror reality, participants will have a difficult time treating it as a real event.

Exercise Evaluation and Critique

Exercise evaluation and critique determines how well the exercise achieved its objectives. This includes organizational-level and individual-level evaluations. Common concerns for evaluation consist of the following needs: to improve the plan, to improve the policies and procedures, to provide additional training, and to overcome staffing problems. A report should be drafted analyzing and critiquing the exercise effort. This report includes recommendations for correcting any problems identified in the report. An organization should not conduct an exercise if there will be no evaluation and critique.

Exercise Follow-up

Exercise follow-up is the most neglected area of the exercising. The lessons learned from the evaluation and critique should be put into action. People have spent time and money to create and execute an exercise, but that investment pays off only if recommendations for improvements are implemented. People should be assigned responsibility for executing each recommendation and given a schedule for when the changes need to be made. Management then monitors the situation to ensure these changes were made. Part of the next exercise should include efforts to test the changes to make sure they work.[9]

DESIGN TEAM

If exercises are done in-house rather than through a vendor, a team must be assembled to design the exercise. The team leader should be someone who has experience with the topic of the exercise, knows the plan to be used in the exercise, and has the time to devote to the design. Other members of the design team should represent the different areas of the organization to be involved in the exercise. The design team will be responsible for determining the exercise objectives, tailoring the scenario to the organization, developing the sequence of events and related messages, helping to create and distribute preexercise materials, and assisting in conducting the preexercise training sessions. Design teams need to have a clear goal and agree on a realistic schedule for preparing the exercise. The leader must schedule regular meetings and monitor the team's progress against its agreed-upon schedule.[10]

Exercise Documents

The design team creates four major documents: the exercise plan, the control plan, the evaluation plan, and the player handbook. The exercise plan is common body of knowledge for everyone involved in the exercise. It serves to guide the design team and helps participants to appreciate and understand the exercise.

Exercise Design Document

Exercise Plan	Control Plan	Evaluation Plan	Player Handbook
Exercise type and purpose Scenario narrative Scope References Objectives Exercise management structure and responsibilities Safety and security	Exercise concept Preexercise player activity Concept for management, control, and simulation Control team staffing Control team training Control team staff responsibilities Control team procedures Communications, logistics, and other support	Exercise concept Preexercise player activity Concept of evaluation management Evaluation team staffing Evaluation team training Evaluation team staff responsibilities Evaluation team responsibilities Support for the evaluation team	Exercise scope Scenario narrative Player procedures and responsibilities Safety and security Communications Reporting Administrative system Recommended preexercise training event Schedule of player exercise briefings Command center procedures

The control plan, which is not for players, sets the rules and explains the roles for the controllers and simulators. Most importantly, it defines the communications, logistics, and administrative structure of the exercise. In other words, the control plan details when events will happen and when certain messages should be delivered.

The evaluation plan provides guidance to evaluators for exercise evaluation procedures, responsibilities, and support. Controllers and simulators will have access to the evaluation plan as well. This plan explains the purpose of the exercise, establishes the basis for evaluation, and provides evaluation criteria that reflect the focus of the exercise. The player handbook details the information that participants need to be involved effectively in the simulation. It serves as the main source of the information present in the player briefing session. The Exercise Design Document table provides a summary of the four documents.[11]

CONCLUSION

Exercises and drills can be used to test and refine emergency management, crisis management, business continuity, and disaster recovery skills. You do not know how well a plan will work or how well your people will perform before you test them. It is better that your plans and people are tested in a nonthreatening exercise or drill than in a real negative event such as an emergency or crisis. Exercises and drills take a commitment of time and finances but are well worth the investment.

See also Benefits of Emergency Management; Business Continuity; Crisis Management; Evacuation in Large and Multiple Tenant Buildings; and Emergency Response Training and Testing: Filling the Gap.

NOTES

1. Federal Emergency Management Agency (FEMA), *Exercise Design* (Washington, DC: U.S. Government Documents Office, 2003), p. 2.1.
2. FEMA, *Exercise Design*, p. 2.17.
3. FEMA, *Exercise Design*, pp. 2.18–2.19.
4. FEMA, *Exercise Design*, pp. 2.5–2.16.
5. FEMA, *Exercise Design*, p. 3.3.
6. FEMA, *Exercise Design*, p. 4.34.
7. FEMA, *Exercise Design*, p. 4.28.
8. FEMA, *Exercise Design*, p. 4.42.
9. FEMA, *Exercise Design*, pp. 3.1–3.11.
10. FEMA, *Exercise Design*, pp. 3.23–3.27.
11. FEMA, *Exercise Design*, p. 3.22.

GUIDANCE APPENDIX

Evaluation Tools

Guidelines, Document Recommendations, and Warning Signs

EVALUATING WHETHER YOU HAVE SILOS

Management can use the following self-survey to determine whether it has a "silo" problem.

To provide a general indication of how entrenched silo mentality is in your organization or department, choose the most accurate response to each of the following ten statements. Be objective as you select the most accurate of three possible responses to each statement:

- True
- Partially true
- Not True

1. Employees have a good understanding of what all other business units do, how they operate, and how they all fit in the big picture.
2. Collaboration is a strong element of the organization's culture.
3. Your peers from other areas of the organization are open to collaborative efforts and joint projects.
4. You believe that silos are detrimental, and you model that belief on an ongoing basis.
5. You encourage your direct reports to collaborate with those outside your business unit.
6. Business units in your organization freely share resources and information with one another.
7. You receive consistent messages from different levels and/or functions within the organization.
8. Your organization has been successful in building commitment for security, business continuity, disaster recovery, and emergency management projects and programs.

9. A vehicle (e.g., work group) exists to facilitate ongoing communication among related functions within your organization (BC/DR/emergency management/security/safety).
10. ALL employees at all levels are aware of the BC, DR, security, and related programs within the organization

SCORING:

Give yourself:

10 points for each TRUE response
5 points for each PARTIALLY TRUE response
0 points for each NOT TRUE response
Maximum possible points = 100

Score	Assessment
90–100	Outstanding. Congratulations to you and your organization. Continue to avoid silo formation.
70–80	Very good. Look for additional improvement opportunities, and avoid further entrenching existing silos.
50–60	Mediocre. Note which questions were answered “no,” and concentrate efforts there.
30–40	Improvement needed. Further assess the situation and develop a plan for positive change.
0–20	HELP!! A great deal of work to be done. Get started now.

Source: Betty A. Kildow

EVALUATING AN EMERGENCY PREPAREDNESS AND RESPONSE PROGRAM

The following survey allows management to assess its emergency preparedness and response program.

Responding to the following twenty-five questions will provide a basic assessment of your organization’s emergency preparedness and response program. Simply answer each question with a yes or no. There is no partial credit, and not knowing an answer equates to a negative response.

1. Is your building equipped with life safety systems, such as emergency lighting, a fire suppression system, a fire alarm system, and fire extinguishers?
2. Do you have an up-to-date emergency preparedness and response plan, one that has been reviewed and updated within the past six months?

3. Does your organization provide each employee with a printed copy of its emergency procedures and post the procedures in all public areas of the building(s), such as reception area, conference rooms, and break rooms?
4. Have you conducted a threat assessment analysis to determine the hazards and threats (natural disasters, technological disasters, human-caused disasters) that may impact your organization?
5. Have you instituted a comprehensive mitigation plan to eliminate or lessen the impact of identified threats?
6. Do you have an evacuation plan? If so, do you review and, as necessary, update this plan not less than annually?
7. Are all employees within your organization familiar with your emergency response plan, and do they know what to do for each type of emergency situation?
8. Does your organization provide new employee orientation to emergency procedures and not less than annual emergency response refresher training (evacuation, bomb threats, medical emergencies) for all employees?

9 In the event of an evacuation, have you determined shutdown procedures to be followed, guidelines for when to follow/not follow the procedures, and designated employees to do so?

10. Do you have employees in each location who have current certification to provide first aid and CPR?
11. Have you designated and trained employee emergency response teams (ERTs) to respond to emergency situations?
12. Do your employees know locations near your building(s) where emergency medical care will be provided after disasters?
13. Have criteria for evacuation and sheltering-in-place been established?
14. Do all employees know how they will be notified if it is necessary to evacuate or shelter-in-place?
15. Is there a system for accounting for employees following an evacuation that includes having assembly areas outside the building?
16. Does the company maintain daily records of visitors, in addition to staff, in the building?
17. Have you conducted a full-scale drill of your evacuation plan within the past six months?
18. Have you set up procedures and lines of communication to provide information to employees after a disaster occurs?
19. Have you established a damage assessment process and identified who will conduct the assessment once public safety officials declare it is safe to reenter the building?
20. Do you have a program in place to help employees address the emotional response to a disaster that impacts your organization and/or its employees?
21. Does your organization have an enforced policy that all visitors to your building(s) be escorted at all times?

22. Do you have a process that ensures that in an emergency or an evacuation drill special assistance will be provided to employees and visitors who have mobility, sight, hearing, or other special needs and have indicated that they require assistance?
23. Have employees been trained to recognize suspicious mail and packages, and do they know what steps to take if one is received?
24. Does your organization encourage employees to prepare their homes and families for disasters?
25. Can you personally name the members of the emergency response team for your area at work?

Give yourself five points for each yes; zero points for each no. How did you do? Although this assessment is not extensive, it provides a good indication of how well your company is doing to prepare to face the next disaster.

125 points	Congratulations to you and your organization—keep up the good work.
100–120 points	Very good. Take another look at the questions to which you responded "no" for areas for enhancement to make your emergency preparedness and response program even better.
55–95 points	Although your organization has made an effort to prepare for disasters, there's room for substantial improvement. Develop a plan to lessen the gap between where you are and where you need to be.
0–50 points	A great deal of work needs to be done—quickly. Get the right people involved, consider getting some outside help, and get started.

Source: Betty A. Kildow

ASSESSING AN ORGANIZATION'S REPUTATION

The following survey can be used to determine how stakeholders perceive your organization's reputation.

Organizational Reputation Scale

The following ten-item scale provides a quick assessment of an organization's reputation. The scale centers on trust, a key element in all evaluations of reputation. The ten items are added together to form the overall reputation score. After the items is a set of directions for scoring the items.

INSTRUCTIONS: Think about YOUR ORGANIZATION'S NAME HERE. The items below concern your impression of the organization. Circle one number for each of the questions. The responses range from 1 = STRONGLY DISAGREE to 5 = STRONGLY AGREE.

1. The organization is basically honest. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

2. The organization is concerned with the well-being of its publics. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

3. I do trust the organization to tell the truth about the incident. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

4. I would prefer to have NOTHING to do with this organization. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

5. Under most circumstances, I WOULD NOT be likely to believe what the organization says. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

6. The organization is basically DISHONEST. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

7. I do NOT trust the organization to tell the truth about the incident. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

8. Under most circumstances, I would be likely to believe what the organization says. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

9. I would buy a product or service from this organization. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

10. The organization is NOT concerned with the well-being of its publics. 1 2 3 4 5
STRONGLY DISAGREE — STRONGLY AGREE

Scoring the Survey

Five items must be reverse coded before creating the overall reputation score: items 4, 5, 6, 7, and 10. When you reverse code, a 1 becomes a 5, a 2 becomes a 4, a 3 stays the same, a 4 becomes a 2, and a 5 becomes a 1.

Once items 4, 5, 6, 7, and 10 are reverse coded, add the ten items together for a final score.

Interpreting the Scores

45 and above	Very positive reputation
38 to 44	Positive reputation
28 to 37	Average/neutral reputation (no strong feelings one way or the other)
23 to 27	Negative reputation
22 and below	Very negative reputation

ASSESSING THE CLIMATE FOR WORKPLACE AGGRESSION IN AN ORGANIZATION

Workplace Aggression Tolerance Questionnaire (WATQ)

The Workplace Aggression Tolerance Questionnaire (WATQ) is designed to assess attitudes about a wide array of workplace aggression behaviors and can be used for benchmarking and risk assessment in organizations. For benchmarking, the WATQ can serve as one form of evaluation for workplace violence training. Prior to training, people can be assessed for their tolerance of aggressive workplace behaviors. Sometime after the training, people can be assessed again to determine whether there has been any change in their tolerance of aggressive workplace behaviors. The evaluation centers on the question, “Are people in the organization perceiving workplace aggression as less appropriate after the interventions have been implemented?”

Although organizations do have workplace aggression policies, only a small percent have any formal risk assessment of workplace aggression. The WATQ provides basic workplace aggression risk assessment by identifying whether particular behaviors and/or departments in an organization have a high tolerance. A high tolerance suggests people would be willing to engage in that form of workplace aggression.

Directions: Please read the following situation and then respond to the statements that follow the story.

Imagine that someone you work with has just completed a performance appraisal/review with the manager. The person believes that the manager has been unfairly critical of his or her job performance—there are some negative comments on the appraisal that the person knows are not accurate.

The person explains to the manager that the negative comments are inaccurate. The manager refuses to make any changes. So, this unfairly negative evaluation goes into the person's record and is seen by others in management. The person knows that the comments could prevent a pay raise and/or promotion.

Below are actions the person might take in response to this meeting. For each action, indicate how appropriate or inappropriate the action would be in the workplace. Mark all your answers by circling the number that corresponds to your evaluation.

The responses range from 1 = VERY INAPPROPRIATE to 5 = VERY APPROPRIATE.

VERY INAPPROPRIATE — VERY APPROPRIATE

1. Fail to return the manager's phone calls. 1 2 3 4 5
2. Say bad things about the manager. 1 2 3 4 5
3. Purposefully work very slowly. 1 2 3 4 5
4. Hit or kick the manager. 1 2 3 4 5
5. Refuse to talk to the manager. 1 2 3 4 5
6. Yell at the manager. 1 2 3 4 5
7. Leave whenever the manager enters the area. 1 2 3 4 5
8. Give the manager dirty looks. 1 2 3 4 5
9. Refuse requests from the manager. 1 2 3 4 5
10. Interrupt the manager when s/he speaks. 1 2 3 4 5
11. Give the manager obscene gestures. 1 2 3 4 5
12. Fail to send the manager information s/he needs. 1 2 3 4 5
13. Spread nasty rumors about the manager. 1 2 3 4 5
14. Show up late to meetings involving the manager. 1 2 3 4 5
15. Deface company property (graffiti, scratches, etc.). 1 2 3 4 5

VERY INAPPROPRIATE VERY APPROPRIATE

16. Fail to warn the manager about a potential problem. 1 2 3 4 5
17. Say bad things about the manager's opinions. 1 2 3 4 5
18. Delay work to make the manager look bad. 1 2 3 4 5
19. Waste needed resources at work. 1 2 3 4 5
20. Fail to deny false rumors about the manager. 1 2 3 4 5
21. Hide needed resources at work. 1 2 3 4 5
22. Sabotage the workplace (break equipment, disrupt heating, etc.). 1 2 3 4 5
23. Steal from the workplace. 1 2 3 4 5
24. Interrupt when the manager tries to speak. 1 2 3 4 5
25. Insult the manager. 1 2 3 4 5
26. Swear at the manager using obscene language. 1 2 3 4 5
27. Mistreat the manager's friends. 1 2 3 4 5
28. Verbally threaten the manager. 1 2 3 4 5

Types of Aggression Measured by Each Item

Physical-Active-Direct	4 (Items 4, 8, 10, and 11)
Physical-Active-Indirect	5 (Items 15, 19, 21, 22, and 23)
Physical-Passive-Direct	3 (Items 3, 7, and 24)
Physical-Passive-Indirect	2 (Items 14 and 18)
Verbal-Active-Direct	4 (Items 6, 25, 26, and 28)
Verbal-Active-Indirect	4 (Items 2, 13, 17, and 27)
Verbal-Passive-Direct	3 (Items 1, 5, and 9)
Verbal-Passive-Indirect	3 (Items 12, 16, and 20)

PANDEMIC PREPAREDNESS EVALUATION

The following survey can be used to determine how well an organization's pandemic preparedness matches with U.S. governmental guidelines.

Mad Cow, Y2K and SARS have had a profound effect on how we view potential threats. Those of us in the disaster recovery industry have particular insights into the differences of real and perceived threats. The CDC has recommended preparedness guidelines for large corporations.

The following section has adopted categories from the CDC preparedness checklist. Information you provide will help supply longitudinal data for realistic preparation. Please CHECK ONE box on the right for EACH of the questions.

	Not Started	In Progress	Completed
BUSINESS			
Identify a pandemic coordinator and/or team with defined roles and responsibilities for preparedness and response planning. The planning process should include input from labor representatives.	□	□	□
Identify essential employees and other critical inputs (e.g., raw materials, suppliers, subcontractors, services/ products, and logistics) required to maintain business operations by location and function during a pandemic.	□	□	□
Train and prepare ancillary workforce (e.g., contractors, employees in other job titles/descriptions, retirees).	□	□	□
Develop and plan for scenarios likely to result in an increase or decrease in demand for your products and/or services during a pandemic (e.g., effect of restriction on mass gatherings, need for hygiene supplies).	□	□	□
Determine potential impact of a pandemic on company business financials using scenarios that affect different product lines and/or production sites.	□	□	□
Determine potential impact of a pandemic pandemic on business-related domestic and domestic and international travel (e.g., quarantines, border closures).	□	□	□

	Not Started	In Progress	Completed
Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources, and make sustainable links.	□	□	□
Establish an emergency communications plan and revise periodically. This plan includes identification of key contacts (with backups), chain of communications (including suppliers and customers), and processes for tracking and communicating business and employee status.	□	□	□
Implement an exercise/drill to test your plan, and revise periodically.	□	□	□
EMPLOYEES AND CUSTOMERS			
Forecast and allow for employee absences during a pandemic due to factors such as personal illness, family member illness, community containment measures and quarantines, school and/or business closures, and public transportation closures.	□	□	□
Implement guidelines to modify the frequency and type of face-to-face contact (e.g., handshaking. seating in meetings, office layout, shared workstations) among employees andbetween employees and customers (refer to CDC recommendations).	□	□	□
Encourage and track annual influenza vaccination for employees.	□	□	□
Evaluate employee access to and availability of health care services during a pandemic, and improve services as needed.	□	□	□
Evaluate employee access to and availability of mental health and social services during a pandemic, including corporate, community, and faith-based resources, and improve services as needed.	□	□	□

	Not Started	In Progress	Completed
Identify employees and key customers with special needs, and incorporate the requirements of such persons into your preparedness plan.	□	□	□
POLICIES TO BE IMPLEMENTED DURING A PANDEMIC			
Establish policies for employee compensation and sick leave absences unique to a pandemic (e.g., nonpunitive, liberal leave), including policies on when a previously ill person is no longer infectious and can return to work after illness.	□	□	□
Establish policies for flexible worksite (e.g., telecommuting) and flexible work hours (e.g., staggered shifts).	□	□	□
Establish policies for preventing influenza spread at the work site (e.g., promoting respiratory hygiene/coughing etiquette, prompt exclusion of people with influenza symptoms).	□	□	□
Establish policies for employees who have been exposed to pandemic influenza, are suspected to be ill, or become ill at the work site (e.g., infection control response, immediate mandatory sick leave).	□	□	□
Establish policies for restricting travel to affected geographic areas (consider both domestic and international sites), evacuating employees working in or near all affected areas when an outbreak begins, and guidance			

	Not Started	In Progress	Completed
for employees returning from affected areas (refer to CDC travel recommendations).	□	□	□
Set up authorities, triggers, and procedures for activating and terminating the company's response plan, altering business operations (e.g., shutting down operations in affected areas), and transferring business knowledge to key employees.	□	□	□
PROTECTION FOR EMPLOYEES AND CUSTOMERS DURING A PANDEMIC:			
Provide sufficient and accessible infection control supplies (e.g., hand hygiene products, tissues and receptacles for their disposal) in all business locations.	□	□	□
Enhance communications and information technology infrastructures as needed to support employee telecommuting and remote customer access.	□	□	□
Ensure availability of medical consultation and advice for emergency response.	□	□	□
COMMUNICATION AND EDUCATION FOR EMPLOYEES			
Develop and disseminate programs and materials covering pandemic fundamentals (e.g., signs and symptoms of influenza, modes of transmission), personal and family protection and response strategies (e.g., hand hygiene, coughing/sneezing etiquette, contingency plans).	□	□	□
Anticipate employee fear and anxiety, rumors, and misinformation, and plan communications accordingly.	□	□	□
Ensure that communications are culturally and linguistically appropriate.	□	□	□
Disseminate information to employees about your pandemic preparedness and response plan.	□	□	□

	Not Started	In Progress	Completed
Provide information for the at-home care of ill employees and family members.	□	□	□
Develop platforms (e.g., hotlines, dedicated web sites) for communicating pandemic status and actions to employees, vendors, suppliers, and customers inside and outside the work site in a consistent and timely way, including redundancies in the emergency contact system.	□	□	□
Identify community sources for timely and accurate pandemic information (domestic and international) and resources for obtaining countermeasures (e.g., vaccines and antivirals).	□	□	□
EXTERNAL ORGANIZATIONS AND COMMUNITY HELP			
Collaborate with insurers, health plans, and major local health care facilities to share YOUR pandemic plans and understand their capabilities and plans.	□	□	□
Collaborate with federal, state, and local public health agencies and/or emergency responders to participate in THEIR planning processes, share your pandemic plans, and understand their capabilities and plans.	□	□	□
Communicate with local and/or state public health agencies and/or emergency responders about the assets and/or services YOUR business could contribute to the community.	□	□	□
Share best practices with other businesses in your communities, chambers of commerce, and associations to improve community response efforts.	□	□	□

Scoring Responses:

0 points for Not Started
1 point for In Progress
2 points for Completed

0 to 33	Not prepared. Your organization needs to focus on pandemic preparation.
33 to 62	Strong progress. Review to see where you scores are still below a 2 to continue preparation.
66	Top score. Your organization is fully prepared according to the CDC.

INFORMATION SECURITY POLICY CONTENT AREAS

Here is a list of the basic points covered in a typical information security policy.

Title. A concise title provides users with a clear understanding of the policy's contents.

Version. A consistent numbering system helps users (and the document's author) determine at a glance whether a policy has been updated. If most of the policies in the manual have a version number of 1.0, then a policy with a version of 1.1 has undergone a minor revision, whereas 2.0 represents a major revision.

Last review date. This is the date that your organization's subject matter experts most recently reviewed the policy, whether they suggested any changes or not.

Publication date. This is the date that the policy was most recently published, in either hardcopy or electronic format.

Expiration date. On this specified date the policy will expire.

Classification. A categorization of the policy document within your organization's overall document classification scheme is helpful.

Owner. This party within your organization is responsible for reviewing, revising, and enforcing each policy.

ISO reference. This is the section of the ISO standard (or any other recognized standard) on which the policy is based.

Associated standards. A list of all standards and guidelines that reference the policy is helpful.

Scope. This is to whom the policy applies. Most likely, all employees, contractors, and business partners will be expected to follow all policies. Still, certain policies could apply exclusively to employees or to contractors.

Reporting violations. There should be a method—or several methods—that your organization's members can use to report a suspected violation of policy.

Noncompliance/penalties. This is a clear statement that explains the repercussions of violating the policy.

Terms and definitions. These are any technical, unique, or ambiguous terms used in the policy.

Body. The topic covered determines the length of the real "meat" of the policy.

Source: Michael Seese.

REQUESTING AN EXCEPTION TO AN INFORMATION SECURITY POLICY

Persons requesting exceptions to policy should complete and submit a form that specifies the following:

- The specific policy that their request violates
- An explanation of what they are requesting, including how it violates policy
- A thorough description of their business process, including details of how the policy interferes with their operations
- A business justification
- The impact to their operations if the exception were not granted
- A list of the alternatives considered and why they were determined to be unacceptable
- A risk assessment, including:
    - The type of data being put at risk
    - Any exposures created if the exception were granted
    - The likelihood that any given vulnerability could be exploited
    - A description of what an attacker could do if he or she exploited the vulnerability created by the exception
    - The impacts to the organization if the vulnerability were exploited
    - Any controls that will be implemented to mitigate the risks

The request is then reviewed. A denial of a request should contain an explanation for the denial. If a request is granted, the expiration date for the exception should be specified.

Source: Michael Seese.

COMMON SIGNS OF SOCIAL ENGINEERING

The following activities should be warnings to workers that a social engineer may be at work:

- Refusal to give *back* adequate information or an explanation
- Expressing a sense of urgency
- Providing names with no context

- Intimidating behavior
- Outright requesting of sensitive information

Source: Michael Seese.

STEPS FOR CONSTRUCTING THE CRISIS SENSING MECHANISM

Step 1: Identify Existing Crisis Sensing Activities

Audit your organization to determine what units are already sensing the environment. You want to avoid re-creating the wheel, so use the existing sensing activities as a foundation for your crisis sensing mechanism. Be sure to review risk assessment, issues management, and stakeholder relationship activities. Ask each organizational unit what it currently does to identify problems/opportunities internally or externally—its scanning activities.

Step 2: Assess the Existing Crisis Sensing Activities

You may need to develop new crisis sensing activities if the existing ones do not form a complete system. If key risk sources are being overlooked, you need to expand the crisis sensing activities. For example, if no effort is made to scan relevant activist groups, add that as a source. Make sure all possible sources you can think of are being scanned.

Step 3: Assess Information Gathering Techniques

Review how the information is being gathered. Pay particular attention to any coding systems used. A common weakness in information collection is a coding system that is too general and misses important details contained in the information. Consider an example of a retail store that codes news stories and blog entries about the organization. A general coding system would simply count the total number of positive and negative comments about the store. Such coding provides a global assessment of the reputation—is the reputation favorable or unfavorable? No insight is given into why the media image is favorable or unfavorable. A specific coding system might include categories such as sales staff, customer service, selection, merchandise quality, value/pricing, store appearance, and parking. The retail store would have separate evaluations for the seven categories. Store managers would know which exact areas of the store's reputation were strong and which needed improvement.

Step 4: Develop Procedures for Funneling Information

A crisis manager or team can neither process information it does not receive nor attend to prodromes it never knew about. Procedures must be developed for routing the information to the crisis manager in a timely fashion. Various parts of the organization will be responsible for different pieces of information. Some organizational units involved in scanning include security, operations and manufacturing, marketing and sales, finance, human resources, legal, customer communications and satisfaction, environmental and safety engineering, public relations/public affairs, engineering, shipping and distribution, and quality assurance. The different units must route their information to the crisis manager, who evaluates it for prodromes. Taking a cue from integrated marketing communication, the organization must share vital incoming information. The crisis manager/team becomes the center of a large crisis sensing mechanism. The crisis manager/team must be treated as a functioning unit that is integrated within the flow of organizational activities and information flow.

Step 5: Establish Evaluative Criteria

Each crisis manager/team must decide how to translate these general criteria into organizational-specific criteria it can use. The crisis manager/team must decide which criteria to use, create any additional criteria that may be needed, and very clearly define the evaluative criteria. Without clear definitions, the criteria cannot be applied consistently by the crisis manager/team. For instance, what is the difference between risk impact ratings of 3, 6, and 9? The criteria must be used consistently if the crisis team is to compare and rank order the prodromes. It takes time to develop precise criteria, but the rewards are well worth the work.

Step 6: Test the Crisis Sensing Mechanism

Developing a crisis sensing mechanism does not mean it works. The system must be tested. Tests are as simple as placing selected information into the various sensing activities and seeing whether that information reaches the crisis manager and how long it takes. The crisis sensing mechanism is a complex communication/information processing system that requires regular checking and refinement in order to maintain and to improve its efficiency.

HOW TO SHELTER-IN-PLACE

The basic steps to sheltering-in-place for a company include the following:

1. Close the business and post signs warning those outside the building.
2. Inform all those in the building, including visitors and customers, of the situation and the reason to shelter-in-place.
3. Shut and lock all windows and doors.
4. Have people assemble in designated rooms and bring the disaster supplies to these locations. The disaster supplies include nonperishable food, water, battery-powered radios, first aid supplies, batteries, flashlights, phones/phone access, garbage bags, duct tape, and plastic. The National Institute for Occupational Safety and Health (NIOSH) recommends a

variety of respirators that can be used during an evacuation to protect people from smoke inhalation.

5. Have people call their emergency contacts to inform them of what is happening.
6. Turn off all heating, ventilation, and/or air conditioning. An employee who has been trained in the proper way to shut down these mechanical systems should do this.
7. Seal the windows and vents with sheets of plastic and duct tape. Ideally the pieces of plastic are precut to fit the openings and employees are preassigned and trained in how to seal the windows and vents.
8. Seal around doors with plastic and duct tape.
9. Turn on the radio or television and listen for further instructions.
10. Once the all clear is given, remove plastic, restart the mechanical system, and go outside of the building until the old, possibly contaminated air in the system has been replaced with fresh, clean air.

Source: American Red Cross, "Shelter-in-Place in an Emergency," online at http://www.redcross.org/services/prepare/0,1082,0_258_,00.html (accessed 5 May 2006).

COMPONENTS OF AN ETHICS AND COMPLIANCE PROGRAM

The U.S. Department of Commerce has identified nine components that are needed for an effective ethics and compliance program:

1. A set of standards and procedures that guides employee conduct and helps stakeholders understand what to expect from a company's employees.
2. A system that holds employees accountable for living up to the program's requirements
3. Clear communication of the program and policies to employees
4. Active monitoring of employee conduct
5. Encouraging employees to seek advice when they have ethics questions
6. Due diligence in hiring employees
7. Encouraging employees to follow the policies and guidelines
8. Management taking appropriate actions when the policies and guidelines are violated
9. Regularly evaluating the program's effectiveness

COMPONENTS OF ANTICORRUPTION POLICIES

Antcorruption policies:

- Must forbid any bribes
- Must specify that intermediaries are not to use any of the money for bribes

- May allow facilitation payments under certain conditions, including payments that are customary and of low value, are approved by senior management, do not violate any laws, are reported immediately, and are recorded in company records
- Must set limits for gifts and entertainment
- Must specify no kickbacks and use accounting and monitoring procedures to ensure policy is not violated
- Must ensure that conflict of interest is to be avoided at all times

WHAT CREATES OUTRAGE IN RISK COMMUNICATION

Outrage can be created or reduced by at least twelve different factors:

1. *Voluntary versus coercive.* Risk bearers are less likely to experience outrage when they expose themselves to a risk rather than having the risk thrust upon them.
2. *Natural versus industrial.* Risk bearers have less of an emotional reaction to natural risks, such as a tornado, than to risks created by other people, such as hazardous waste.
3. *Familiar versus unfamiliar.* Risk bearers perceive familiar things as less risky than unfamiliar things.
4. *Memorable versus not memorable.* Risk bearers rate the risk higher when it is linked to some memorable event than when it is a little known event. Bhopal is memorable, increasing the perception of risk for similar pesticide production facilities.
5. *Dreaded versus not dreaded.* Risk bearers rate risk higher when that risk is linked to a dreaded outcome such as cancer.
6. *Chronics versus catastrophic.* Risk bearers rate risks they face every day, such as driving, less seriously than catastrophic events, such as airplane crashes.
7. *Knowable versus unknowable.* Risk bearers fear the unknown more than the known. A new risk should generate more outrage than a well-known risk.
8. *Control versus not in control.* Risk bearers feel more secure when they have the ability to control or regulate the risk. Again, the idea of driving versus flying in a plane fits well. People can control the car when they are driving but not the plane when a pilot is doing the flying.
9. *Fair versus unfair.* Risk bearers experience greater outrage from a risk if they perceive their burden from the risk carries a greater price than that of other people.
10. *Morally irrelevant versus morally relevant.* Risk bearers experience greater outrage if the risk is linked to immoral actions such as cutting corners to make profits than if the risk is related to some moral good such as curing a disease.

11. *Trustworthy versus untrustworthy.* Risk bearers experience less outrage if they trust the experts involved in the risk communication effort than if they lack trust in those experts.
12. *Responsive versus unresponsive.* Risk bearers feel greater outrage when the company responsible for the risk is unresponsive to their concerns.

Source: Peter M. Sandman, "Risk Communication: Facing Public Outrage," online at http:// www.du.edu/~scbeckma/EPM4700/outrage.htm (accessed 27 Feb. 2007).

SPOKESPERSON TASKS FOR CRISIS MANAGEMENT

A spokesperson has four main tasks: (1) appear pleasant on camera, (2) answer questions effectively, (3) present crisis information clearly, and (4) handle difficult questions.

1. To appear trustworthy and in control, a spokesperson must maintain consistent eye contact (eye contact at least 60 percent of the time), use hand gestures to emphasize points, avoid a monotone by varying vocal qualities, have an expressive face, and avoid too many vocal fillers such as "uhs" or "ums."
2. An effective answer to a question is one that answers the question that is asked.
3. A spokesperson's answers must be clear and easy for the reporters to understand. This means avoiding jargon and technical terms.
4. A spokesperson needs to recognize the tough question and respond strategically. Any practice sessions should include some tricky questions.

BASIC GUIDES FOR USING PASSWORDS

1. Do not use words found in the dictionary, even those from another language.
2. Different systems should have different passwords, not just one.
3. Use upper- and lower-case letters.
4. Use a combination of numbers, special characters, and letters.
5. Do not use passwords derived from personal information such as birthdays.
6. Use a mnemonic to help you remember a password.

Source: Mindi McDowell, Jason Rafail, and Shawn Hernan, "Choosing and Protecting Passwords," 2004, online at http://www.us-cert.gov/cas/tips/ST04-002.html (accessed 5 March 2007).

SPYWARE SYMPTOMS

1. Endless pop-ups
2. Redirection to web sites other than the ones you selected

3. Appearance of new toolbars on your web browser
4. Appearance of new icons along the bottom of your computer screen
5. The home page of your browser changes
6. Different search engine appears when you click your search icon
7. Certain keys do not work in your browser
8. Appearance of random Window error messages
9. Noticeable drop in your computer's processing speed

Source: Mindi McDowell and Matt Lytle, "Recognizing and Avoiding Spyware," 2004, online at http://www.us-cert.gov/cas/tips/ST04-016.html (accessed 5 March 2007).

INFORMATION SECURITY BASIC GUIDANCE

The U.S. Department of Homeland Security has issued a set of guidelines for businesses. The recommendations cover employees and management.

Employees

1. Require the use of strong passwords.
2. Require that passwords be changed every forty-five to ninety days.
3. Never give your user name or password to anyone.
4. Never open e-mail attachments from people you do not know.
5. Get permission from the company's IT department before installing any of your own software or hardware.
6. Keep electronic and physical backups of the most important work.
7. Report suspicious activities or problems to the IT department.

Management/IT Department

1. Monitor, log, and evaluate any attempts to enter your network or system.
2. Create and reinforce clear policies for how employees are to use the information technologies.
3. Download patches regularly.
4. Create a layered defense that includes technical, organizational, and operational controls.
5. Use technical defenses such as firewalls, Internet content filters, and intrusion detection systems.
6. Update antivirus software regularly.
7. Change the manufacturer's default passwords.

SAMPLE CRISIS MANAGEMENT PLAN ELEMENTS

Generic Components of a Crisis Management Plan

1. Cover page
2. Introduction

3. Acknowledgments
4. Rehearsal dates
5. Crisis management team list
6. CMT contact sheet
7. Secondary contact sheet
8. Crisis risk assessment
9. CMT strategy worksheet
10. Stakeholder contact worksheet
11. Business continuity plan reference
12. Crisis control center
13. Postcrisis evaluation tools

Incident Report

Date and Time Incident Was Reported: Initial Report___

Individual Reporting the Incident: Follow-up ___

How to Contact the Reporting Individual:

Description of the Incident:

Exact Location of the Incident:

List the Personnel and Units Responding to the Incident:

Describe What Is Being Done to Address the Incident and by Whom:

List Any Follow-up Action That Is Needed:

Detail the Damage Inflicted by the Crisis:

Date and Time the Crisis Team Was Notified:

What Other Units (i.e., fire department security, EMTs, etc.) Were Contacted and When?

Crisis Management Team Strategy Worksheet

Stakeholder(s) Targeted by the Message:

- Consider the status of the current relationship with each stakeholder.
- Review the primary organizational performance expectations of each stakeholder.
- LIST STAKEHOLDER(S) HERE:

Goal of the Message:

Attach a copy of the actual message to this sheet.

Stakeholder Contact Worksheet

Date: Time:

Organizational Member Handling the Inquiry:

Channel Used to Contact the Organization:

Stakeholder's Classification (i.e., media, stockholder, community leader, etc.):

Inquiring Person's Name and Title:

Inquiring Person's Organizational Affiliation:

How to Reach the Inquiring Person:

Question/Inquiry:

Response:

Any Follow-up Needed: If So, by Whom:

When:

INITIATING EMERGENCY NOTIFICATION COMMUNICATION

Notification during disruptive events such as crises, disasters, and emergencies is critical to safety. This entry reviews key aspects of an effective notification system: initiating emergency notification, reaching the right people with the right message at the right time, delivering and receiving messages, communication efficiency, and ease of use.

Initiating Emergency Notification

The first task facing the disaster manager is to initiate or accelerate the information flow. This poses a formidable challenge if the communication center or emergency operations center has been damaged or communication lines are down. Automated notification simplifies the task by reducing the number of messages that must be initiated; it allows the coordinator to issue a single message to an entire list of people—whether that group consists of employees, customers, parents of schoolchildren, first responders, or reporters. The chances of initiating and delivering messages successfully are much greater if the initiator has to send only five messages instead of five thousand. There should be multiple ways to initiate a message. At the very least, disaster coordinators need to be able to access and use their notification system through the Internet and by telephone without being at a particular computer or telephone to initiate a message. The system should also be able to deliver messages from multiple initiators. Managers need to delegate authority to several associates so that emergency notification does not fail should one person be incapacitated or unavailable.

Reaching the Right People with the Right Message at the Right Time

Nearly as important as reaching all the critical audiences is sending messages only to those who need to receive them. Sending extraneous messages in times of emergency can have serious unintended consequences, including chaos and crowding at the disaster site, an influx of unwanted phone calls, and even mass panic. To channel messages correctly, your messaging tools need to have the capacity for unlimited groups and subgroups of target audiences. Crisis communicators may have to poll employees from the seventh floor to make sure they were all safely evacuated from a fire; instruct employees in the network services division to report to a backup site the next morning; or recall certain ambulance crews but not others. Relationships between list members must be identifiable to allow crisis communicators to make selections based on these relationships—for example, contacting "all the senior managers and executives in the Chicago office."

Delivering and Receiving Communication

Communication flows constantly in two directions during a crisis: incoming and outgoing messages, information, and meta-messages. Usually, just sending out messages is not enough; the crisis manager must learn who has been contacted successfully and, sometimes, what the responses are. An automated notification system can be a great mechanism for receiving and reporting such responses. To facilitate two-way communication, the notification system should be able to receive an active response, such as a keypad entry, to confirm successful delivery of a message. The notification system should also be capable of surveying or polling recipients. For example, if first responders are being notified, the coordinator's message might ask them to press 1 if they are already at the disaster site, press 2 if they are on their way there, and press 3 if they are unavailable to respond to the emergency. Reports of all message delivery attempts, confirmations, and polling results should be easily available by Internet and fax, and summary reports need to communicate the overall picture quickly. Detailed reports show where individual follow-up is needed.

Communication Efficiency

The many automated notification services on the market today vary widely in terms of capacity, data security, and cost. With those major considerations always in mind, the greatest communications utility for a business obviously comes from an automated system having features and functionality that best match its communication needs in a crisis. Advanced features, such as conference calling and geographic targeting (which allows messages to be automatically delivered to all residents in a specific geographic area), are important to consider, because they maximize communication options for a crisis manager. Feature-rich systems are more likely to overcome common communication obstacles, such as phone line jams or loss of Internet connectivity. This collection has mentioned the value of having preplanned scenarios and premade statements to ensure expediency and message quality in the middle of a disaster. Many automated systems offer message libraries, in which created messages can be stored, as well as the functionality to create crisis scenarios connecting specific prepared messages with the exact group(s) they will be sent to when an incident occurs.

Ease of Use

An automated notification system should be easy to use without extensive training. Just as crisis communicators should not be spending hours making phone calls, they should not be trying to remember complicated command sequences or searching for user manuals. Stress and anxiety during a crisis make communication difficult, and an automated notification system needs to reduce the stress, not add to it. Ideally, all functional areas of a crisis management team—operations, security, legal, communications (public relations), management, and finance—will be able to utilize an automated system for their own unique communication requirements. Crisis management teams have other critical tasks besides sending and receiving messages. But, as we have seen, one-on-one communications are so stressful and time-consuming under the best of circumstances that they can delay a coordinated response and even lead to loss of property or life. A quality automated notification/mass notification system greatly reduces time spent on communications and frees emergency personnel to deal with crisis mitigation, response, and recovery work. Being able to initiate a few messages and receive hundreds or thousands of responses formatted in a readable report just a few minutes later is an enormous time-saver. An automated notification system is an ideal way to fill the information void quickly, while carefully delivering the right message to the right audience. The following table summarizes this information.

After a message has been initiated, it must be delivered to everyone on the delivery list. There are two important issues: whether the messages will arrive and when they will arrive. To maximize the likelihood that messages will be delivered in a timely manner, your emergency notification system should be able to send messages to all types of contact devices—phone, cell, fax, computer (e-mail and instant messaging), pager, PDA (including BlackBerry)—and in as many formats as possible (voice, text, short message service [SMS]). The notification system should permit multiple contact paths for each person on the list, and allow

Communication Challenge	Automated System
Heavy demand for information (volume)	• Able to send hundreds, or even thousands, of messages in seconds
Communication systems or contact paths are unavailable	• Utilizes multiple communication networks and paths (not all channels will be damaged)
	• Built with redundant, geo-dispersed systems that can survive regional failures
Severe time constraints; little time for analysis or investigation	• Leverages speed and delivery reliability to both disseminate information quickly and give decision makers more time to make choices
Crisis manager's normal location is inaccessible	• Notification system and contact data are accessible from anywhere
	• Administrator can delegate authority to an alternate whose office is intact
Personnel are scattered	• Multiple communication pathways maximize chances of finding and reaching your audience
One-on-one communication takes too long	• Thousands of calls can be placed in a few seconds/minutes; some systems offer conference calling and geographic targeting
Collecting information from audience is difficult	• Automated polling and real-time summaries of polling data
Inconsistent, inaccurate, or incomplete information is issued	• Identical recorded or text messages allow accurate and consistent information flow; speed and volume of automation allow rumors to be quashed quickly

Source: Robert Chandler.

a different order for each list member. (For example, member 1 might designate cell phone first, then e-mail, then fax; member 2 might choose work phone first, then home phone, then pager.) The notification system must be able to make unlimited attempts to contact each person on the list, until there is confirmation of receipt of the message or the message update.

RESOURCE APPENDIX

BOOKS

Information and Physical Security

Bailes, Alyson J. K., and Frommelt, I., ed., *Business and Security: Public-Private Sector Relationships in a New Security Environment.* Stockholm, Sweden: SIPRI, 2004.

Borodzicz, Edward, *Risk, Crisis and Security Management.* Indianapolis, IN: Wiley Publishing, 2005.

Broder, James F., *Risk Analysis and the Security Survey, Third Edition.* Burlington, MA: Butterworth-Heinemann, 2006.

Calder, Alan, *A Business Guide to Information Security.* London, UK: Kogan, 2005.

Cumming, Neil, *Security: A Guide to Security System Design and Equipment Selection and Installation, Second Edition.* Burlington, MA: Butterworth-Heinemann, 1994.

Dalton, Dennis, *Security Management: Business Strategies for Success.* Burlington, MA: Butterworth-Heinemann, 2006.

Ghosh, Anup K., *Security & Privacy for E-Business.* New York: Wiley Publishing, 2001.

Gouin, Brian, *Security Design Consulting: The Business of Security System Design.* Burlington, MA: Butterworth-Heinemann, 2007.

Kairab, Sudhanshu, *A Practical Guide to Security Assessments.* Boca Raton, FL: Auerbach, 2004.

Khairallah, Michael, *Physical Security Systems Handbook: The Design and Implementation of Electronic Security Systems.* Burlington, MA: Butterworth-Heinemann, 2005.

Kildow, Betty A., *Frontdesk Security and Safety: An On-the-Job Guide to Handling Emergencies, Threats, and Unexpected Situations.* New York: AMACOM, 2004.

Kovacich, Gerald L., *The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program, Second Edition.* Burlington, MA: Butterworth-Heinemann, 2003.

McCarty, Mary Pat, and Campbell, Stuart, *Security Transformation: Digital Defense Strategies to Protect Your Company's Reputation and Market Share.* New York: McGraw-Hill, 2001.

McCrie, Robert, *Security Operations Management, Second Edition.* Burlington, MA: Butterworth-Heinemann, 2006.

Peltier, Thomas R., *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition.* Boca Raton, FL: Auerbach, 2004.

Peltier, Thomas R., *Risk Management for Business and Security.* Boca Raton, FL: Auerbach, 2008.

Purpura, Philip, *The Security Handbook, Second Edition.* Burlington, MA: Butterworth-Heinemann, 2002.

Wylder, John, *Strategic Information Security.* Boca Raton, FL: Auerbach, 2003.

Security-Related Topics

Apgar, David, *Risk Intelligence: Learning to Manage What We Don't Know.* Cambridge, MA: Harvard Business School Publishing, 2006.

Coombs, W. Timothy, *Code Red in the Boardroom: Crisis Management as Organizational DNA.* Westport, CT: Praeger, 2006.

Coombs, W. Timothy, *Ongoing Crisis Communication: Planning, Managing, and Responding, Second Edition.* Thousand Oaks, CA: Sage, 2007.

Crouhy, Michel, Galai, Dan, and Mark, Robert, *The Essentials of Risk Management.* New York: McGraw-Hill, 2005.

Entis, Phyllis, *Food Safety: Old Habits and New Perspectives.* Washington, DC: ASM Press, 2007.

Fleisher, Craig S., and Blenkhorn, David L., eds., C*ontroversies in Competitive Intelligence: The Enduring Issues.* Westport, CT: Praeger, 2003.

Hoffman, Bruce, *Inside Terrorism.* New York: Columbia University Press, 2006.

Ledlow, Gerald R., Johnson, James A., and Jones, Walter J., C*ommunity Preparedness and Response to Terrorism:* Vol I, *The Terrorist Threat and Community Response.* Westport, CT: Praeger, 2005.

McFall, Kathleen, *Ecoterrorism: The Next American Revolution?* Portola, CA: High Sierra Books, 2005.

McGonagle, John J., and Vella, Carolyn M., *Protecting Your Company Against Competitive Intelligence.* Westport, CT: Quorum Books, 1998.

Mitnick, Kevin, and Simon, William, *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, IN: Wiley Publishing, 2002.

Odiorne, George S., *Management and the Activity Trap.* New York: Harper & Row, 1974.

Sikich, Geary W., *Integrated Business Continuity: Maintaining Resilience in Times of Uncertainty.* Tulsa, OK: PennWell Publishing, 2003.

White, Jonathan R., *Terrorism and Homeland Security, Fifth Edition.* Mason, OH: Wadsworth Publishing, 2005.

MAGAZINE AND JOURNAL ARTICLES

Chandler, Robert C., "Managing Ethical and Regulatory Compliance Contingencies: Planning and Training Guidelines," *Contingency Planning and Management 2000 Proceedings*. Flemington, NJ: Witter Publishing, 2000, pp. 6–7.

Chandler, Robert C., and Wallace, J. D., "Brief Results of the Pepperdine University Ethical Misconduct Disaster Recovery Preparedness Survey," *Disaster Recovery Journal*, 14, 3 (2001), 21–22.

Sikich, Geary W., "What Is There to Know About a Crisis," *John Liner Review*, 14, 4 (2001).

Sikich, Geary W., "Hurricane Katrina: Nature's 'Dirty Bomb' Incident? *Continuity Central*, Lead Article, 30 Sept. 2005.

Sikich, Geary W., "Business Continuity as a Strategic Initiative," *The Business Continuity Journal*, 1, 1 (2006).

Sikich, Geary W., and Stagl, John M., "Are We Missing the Point of Pandemic Planning?" *Continuity Central*, Dec. 2005.

MAGAZINES

Business Continuity Insights

Presents articles written by experts in the field on a variety of business continuity and business security topics. It is a monthly publication and the subscription is free. You can access a subscription at http://www.continuityinsights.com/Magazine/Magazine_Subscribe.html. The magazine's web site (http://www.continuityinsights.com/) offers a searchable archive of past articles.

CIO

Has a target audience of chief information officers and high-level IT executives. People can apply for a free subscription; those who do not qualify must pay for it. An online subscription form must be completed to determine eligibility for a free subscription at http://www.cio.com/subscription-services.

CPM

This publication has a subscription fee. According to its web site, "Over the past year, *CPM* has closely monitored the business continuity profession and its need to integrate with other disciplines. Earlier this year, we introduced the concept of *operations assurance*, which advocates a closer relationship with business continuity, security, emergency management, risk management, and other critical activities, all under the umbrella of good corporate governance. *CPM* 's readers told us this is an important and strategic direction for their companies. To further develop this important concept in the evolution of business and government continuity of operations, we will provide our readers with the most useful, thought-provoking information and analysis, in a more focused and timely medium." See http://www.contingencyplanning.com/magazine/index.aspx.

CSO

According to its own description, *CSO* "has been serving the information needs of top security executives since 2002. Our loyal audience regularly turns to *CSO* for up-to-date security best practices and strategic management issues through *CSO* magazine, CSOonline.com and CSO Executive Programs." People can apply online for a free subscription to *CSO* or to its newsletter at http://www.csoonline.com/read/.

Disaster Recovery Journal

Provides articles written by experts on a variety of disaster recovery, business security, and business continuity topics. Subscription is free for online delivery and has a small fee for print copies. Subscription information can be accessed at https://www.drj.com/account/index.php.

Security Dealer

Primarily for those involved in selling security systems. It does provide insight into new and developing trends in security services. See http://www.securityinfowatch.com/cover/security-dealer/1SIW.

Security Management

An award-winning magazine published by ASIS International, the preeminent international organization for security professionals. There are reduced fees for ASIS International members. The magazine's web site includes a searchable archive. The articles are written is very accessible manner. Can be found at http://www.securitymanagement.com/.

Security, Technology & Design

Primarily written for security executives. Its content includes both physical and information security and covers access control, video technology, and network-centric applications of IP-based video and ID/data management. See http://www.securityinfowatch.com/cover/security-technology-design/2SIW.

NEWSLETTERS

@Risk: The Consensus Security Alert

"The Critical Vulnerability Analysis and the Security Alert Consensus have merged to become @RISK: The Consensus Security Alert. Delivered every Monday morning, @RISK first summarizes the three to eight vulnerabilities that matter most, tells what damage they do and how to protect yourself from them, and then adds a unique feature: a summary of the actions 15 giant organizations have taken to protect their users. @RISK adds to the critical vulnerability list a complete catalog of all the new security vulnerabilities discovered during the past week. Thus in one bulletin, you get the critical ones, what others are doing to protect themselves, plus a complete list of the full spectrum of newly discovered vulnerabilities. This is also the subscription list that receives SANS Flash Alerts when they come out two or three times a year." Can be found at http://www.sans.org/newsletters/#newsbites.

CIO Newsletters

CIO has a range of newsletters available. *Advice and Opinion* provides the week's top advice and opinion postings. *CIO Careers* offers advice for careers as well as job listings. *CIO ERP* is a CIO's monthly guide for enterprise resource planning. *CIO Enterprise* provides enterprise-level technology information, news, and tools. *CIO Information Security* provides security news and information the CIO needs to know. *CIO Insider* is a guide to the latest from CIO.com covering management, technology, and your career. *CIO Leader* give updates, insights, and advice from CIO.com on your career, as well as practical tips for effective leadership and management. *CIO News Watch* reviews the week's top news stories. *CIO Open Source* is a monthly peek at what's happening in the open source realm. *CIO Research Update* gives highlights of CIO's most recent IT research. *CIO SOA* is a resource for service-oriented and enterprise architecture. *CIO Tech Poll* reports the results of CIO quarterly surveys covering IT's overall health as well as spending and trends. *CIO Whitepapers* provides information about new and upcoming white papers. *CIO Wireless* reports information on emerging wireless technologies and infrastructure, and *Webcast Roundup* is a recap of CXO Media's sponsored on-demand video series. All of the newsletters are free with registration. Can be found at http://www.cio.com/newsletters.

Continuity E-guide

E-mailed once a week to subscribers. It provides summaries of articles on a wide range of business continuity, crisis management, and emergency management topics that are collected online. The reader can click on the full articles and even see the original sources of the material. Can be found at http://www.disaster-resource.com/newsletter/subpages/signup_page.htm.

CPM-Global Assurance

Bills itself as "the one resource that offers it all: analysis, best practices, advice and the contingency planning news. This monthly e-newsletter provides you with in-depth articles authored by the industry's best, case studies, white papers, Q&As, national and international news and product and service offerings. The *CPM Industry Insider* is a great way to stay abreast on the important issues making industry headlines. This monthly e-newsletter offers a quick read of the most important news stories of the month." Can be found at http://www.contingencyplanning.com/magazine/index.aspx.

E-News

Published by *Security Management*. This online newsletter provides short articles on a variety of topics related to physical security including travel safety, background checks, and perimeter security. Can be found at http://www. security management.com/.

Enterprise Strategies

"*Enterprise Strategies* newsletters provide real-world business and technology information for managers of large, high-volume-transaction, high-availability, high-performance computer systems and infrastructures. We offer the latest industry news, analyst and user perspective, and commentary on the latest enterprise, security, and storage trends and technologies. From getting the most out of your system to preparing for security breaches, *Enterprise Strategies* newsletters provide the information and insight to cost-effectively manage your IT resources." See http://esj.com/About_Us/default.aspx.

OUCH!

"OUCH! is the first consensus monthly security awareness report for end users. It shows them what to look for and how to avoid phishing and other scams plus viruses and other malware—using the latest attacks as examples. It also provides pointers to great resources like the amazing Phishing Self-Test. 460 organizations, large and small, helped make it a useful service. More than 100 security officers check each issue for accuracy, and readability before it is distributed to the community." Can be found at http://www.sans.org/newsletters/#newsbites.

SANS NewsBites

"SANS NewsBites is a semiweekly high-level executive summary of the most important news articles that have been published on computer security during the last week. Each news item is very briefly summarized and includes a reference on the web for detailed information, if possible." Can be found at http://www .sans.org/newsletters/#newsbites.

WEB SITES

Business Continuity and Disaster Recovery

http://www.contingencyplanning.com/
This is the home page for the Contingency Planning & Management Group. "The Contingency Planning & Management Group (CPM) is your source for information and strategic advice on business continuity, emergency management and security issues." The site provides access to its two e-newsletters: *CPM Global Assurance and CPM Industry Insider.* Registration is required to access and receive the newsletters. There is a searchable archive as well. "Each of our

electronic newsletters delivers critical information straight to your inbox to help you do your job—and do it better. The CPM Group offers two conferences per year that cover business continuity and security."

http://www.continuityinsights.com/
This is the home page for Business Continuity Insights. The site provides information about business continuity and business security. Resources include white papers, news, podcasts, presentations, and the archive for *Business Continuity Insights* magazine. Business Continuity Insights presents an annual meeting.

http://www.disaster-resource.com/index.htm
This is the home page for Disaster-Resource.com. This site provides resources for those involved in business continuity, crisis management, and emergency management. "Whether you are a senior executive looking for an industry overview, an experienced manager searching for the latest trends, or a new contingency planner in need of the basics, you will find the GUIDE to be the most comprehensive source for crisis/emergency management and business continuity information. The online DISASTER RESOURCE GUIDE is set up to help you find information, vendors, organizations and many resources to help you prepare for (mitigate) or recover from any type of natural or other type of disaster. The GUIDE is to help you keep your business running, your government agency operational, no matter what!" The site allows you to search for products, services, and articles related to business continuity, crisis management, and emergency management. The articles are collected from variety of online sources. People can also subscribe to a newsletter, *Continuity e-guide*.

http://www.drii.org/DRII/
DRI International was founded in 1988 as the Disaster Recovery Institute in order to develop a base of knowledge in contingency planning and the management of risk. DRI International administers educational and certification programs for those engaged in the practice of business continuity planning and management.

http://www.drj.com/
This is the home page for *Disaster Recovery Journal*. The site provides a variety of tools for disaster recovery and business continuity including a toolbox, glossary, and planning model. The site archives news articles and its *Disaster Recovery Journal*. *DRJ* provides two conferences each year.

http://www.idra.com/index.htm
International Disaster Recovery Association is an association of users, researchers, educators, and vendors having a special interest in the voice, data, image, and sensory telecommunications aspects of contingency planning, business continuation, disaster recovery, and restoration. IDRA's mission statement is "To maintain adequate voice, data and image telecommunication services during periods of extraordinary activity and interruptions in normal operations." IDRA holds

workshops, seminars, and multiday conferences at which all topics and exhibits devoted to telecommunications disaster recovery.

Corruption

http://www.iccwbo.org/policy/anticorruption/
This web site is operated by the Anti-Corruption Commission of the International Chamber of Commerce™ (ICC). The Anti-Corruption Commission seeks to "encourage self-regulation by business in confronting issues of extortion and bribery, and to provide business input into international initiatives to fight corruption." The web site details what corruption is, how it harms people, and the ways organizations can fight corruption. There are links to important international anticorruption conventions such as the UN Convention against Corruption, the OECD Anti-Bribery Convention, and the ICC rules of conduct.

http://www.transparency.org/
This is the home page for Transparency International, "the global civil society organisation leading the fight against corruption, [which] brings people together in a powerful worldwide coalition to end the devastating impact of corruption on men, women and children around the world. TI's mission is to create change towards a world free of corruption." This is another resource to consult for information about corruption and ways to combat it. The site includes the global corruption barometer, which provides detailed information annually about corruption in various countries.

http://www.weforum.org/en/initiatives/paci/index.htm
This part of the World Economic Forum's web site is dedicated to its "Partnering Against Corruption Initiative." It provides a discussion of the program and links to other sites dedicated to reducing corruption. "The World Economic Forum is an independent international organization committed to improving the state of the world by engaging leaders in partnerships to shape global, regional and industry agendas. Incorporated as a foundation in 1971, and based in Geneva, Switzerland, the World Economic Forum is impartial and not-for-profit; it is tied to no political, partisan or national interests. The World Economic Forum is under the supervision of the Swiss Federal Government."

Counterintelligence

http://www.ncix.gov/
This web site contains information provided by the Office of the National Counterintelligence Executive (ONCIX). ONCIX is part of the Office of the Director of National Intelligence and is staffed by senior counterintelligence (CI) and other specialists from across the national intelligence and security communities. ONCIX develops, coordinates, and produces the following: annual foreign

intelligence threat assessments and other analytic CI products; annual national CI strategy for the U.S. government; priorities for CI collection, investigations, and operations; CI program budgets and evaluations that reflect strategic priorities; in-depth espionage damage assessments; and CI awareness, outreach, and training standards policies. The site provides resources on counterintelligence and corporate espionage. Security personnel can learn about new threats, especially international threats related to corporate espionage.

Countersurveillance

http://www.abraxascorp.com/default.asp
This is the web site for Abraxas Corporation, a company specializing is risk mitigation technology. Its countersurveillance work centers around TrapWire®, a software program that identifies suspicious computer activity and helps to prevent outside attacks.

http://www.adt.com/wps/portal/adt/
This is the web site for ADT, a provider of security products and services for homes and businesses. ADT has been in existence since 1874 and is the leading provider of electronic security systems in the United States. The web site provides information on how its video surveillance can be used for countersurveillance.

http://www.brinksbusinesssecurity.com/
This is the web site for Brink's Business Security. Brink's has been in business since 1859 and has a strong connection to the security industry in the United States. Brink's provides a large array of security services and equipment. Countersurveillance is one of the applications for its products and services.

http://www.questinvestigations.net/
This is the web site for Quest Consultants International. It provides a range of information and physical security services including countersurveillance. Quest was founded in 1996. The bulk of its employees are veteran ex-FBI agents.

http://www.spybusters.com/spybuster_tips.html
This web site borders on the paranoid but provides interesting information about ways people will try to steal data, including eavesdropping through phone taps and bugging rooms. Tips and equipment for counterespionage are discussed.

Drug Testing

http://www.usdoj.gov/dea/demand/dfmanual/index.html
This link is for the Guidelines for Drug-Free Workplace developed and maintained by the U.S. Drug Enforcement Administration (DEA). The guidelines are useful to any organization that has or is developing a drug testing program. The program details the laws and regulations related to drug testing and how to create an effective drug testing program.

Ecoterrorism

http://www.cdfe.org/ecoterror.htm
This web site explains ecoterrorism and is overseen by the Center for the Defense of Free Enterprise. The site describes what ecoterrorism is, why it is illegal, and some of the major groups involved in ecoterrorism.

Employee Background Checks

http://www.uschamber.com/sb/screening/default.htm?n=tb
This part of the U.S. Chamber of Commerce Small Business web site provides details on employee screening programs. It also includes information on drug screening programs and offers, for a price, a tool kit for employee screening.

Ethics and Compliance

http://www.theecoa.org//AM/Template.cfm?Section=Home
This is the home page for the Ethics & Compliance Officer Association web site. It has limited resources for nonmembers. There is a code of conduct for ethics and compliance officers along with information about education events and training. The organization seeks to create a discussion among its members about the vital issues confronting ethics and compliance officers.

Food Security

http://www.fda.gov/ora/training/orau/FoodSecurity/startpage.html#
This link connects to the Food and Drug Administration's food security awarenss program. The web site provides training free of charge. It is a useful resource for any organization involved in food production and processing. It can be used as part of a larger organizational effort to educate all employees about the need and procedures for food safety.

http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Security_Guidelines/index.asp
This web site is part of the United States Department of Agriculture's Food Safety and Inspection Service (FSIS) and provides information on food defense and emergency response. There are resources for consumers and organizations, with the bulk of the material designed for organizations. Topics include details for developing food security plans, sample food security plans, and emergency guidance for retail food establishments.

General Security

http://www.csoonline.com/read/
This is the home page for *CSO* magazine. The site provides a searchable archive of *CSO* articles as well as podcasts and white papers.

http://www.osac.gov/ResourceLibrary/index.cfm?display=type&type=1003
This web site provides links to a variety of security-related documents developed by governmental sources. Topics include traveling abroad, crisis management, emergency preparedness, and food security.

http://www.securityfocus.com/
This web site provides articles on a variety of security-related topics. The site has a search engine. At the site people can register for the *SecurityFocus* newsletter.

http://www.securityinfowatch.com/
This web site lists a variety of other resources for those interested in security. It is a clearinghouse of security information that includes a search engine.

Information Security

http://www.asisonline.org/
According to the web site, "Founded in 1955 as the American Society for Industrial Security (ASIS), the organization officially changed its name in 2002 to ASIS International. This new name preserves our history while better reflecting the growth and expansion of the society to more than 35,000 members around the world, covering a wide array of services and specialties within the security industry." ASIS offers three certifications: Certified Protection Professional™, Professional Certified Investigator™, and Physical Security Professional™.

http://www.cerias.purdue.edu/
This is the home page for the Center for Education and Research in Information Assurance and Security (CERIAS). CERIAS provides free access to research conducted by members of these groups. CERIAS describes itself as "one of the world's leading centers for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure. CERIAS is unique among such national centers in its multidisciplinary approach to the problems, ranging from purely technical issues (e.g., intrusion detection, network security, etc.) to ethical, legal, educational, communicational, linguistic, and economic issues, and the subtle interactions and dependencies among them."

Research by CERIAS covers eight main topics: risk management, policies, and laws; trusted social and human interactions; security awareness, education, and training; assurable software and architectures; enclave and network security; incident detection, response, and investigation; identification, authentication, and privacy; and cryptology and rights management.

http://www.cio.com/topic/1419/Security
This is the home page for CIO, a site dedicated to chief information officers. According to the web site: "Serving chief information officers and other IT leaders, CIO.com, CIO magazine, CIO Executive Programs, CIO Custom Solutions Group and the CIO Executive Council are produced by CXO Media, an award-winning

business unit of International Data Group. CXO Media also produces sister publications CSO magazine and CSOonline.com, for chief security officers and other security executives. Starting in 1987 with CIO magazine, CIO's portfolio of properties has grown to provide technology and business leaders with insight and analysis on information technology trends and a keen understanding of IT's role in achieving business goals. The magazine and website have received more than 160 awards to date, including two Grand Neal Awards from the Jesse H. Neal National Business Journalism Awards and two National Magazine of the Year awards from the American Society of Publication Editors."

http://csrc.nist.gov/focus_areas.html#st
This is the web site for the Computer Security Resource Center for the National Institute of Standards and Technology. The web site contains information on four areas: cryptographic standards and applications, security testing, security research/emerging technologies, and security management and assistance.

http://www.esj.com/index.aspx
This is the home page for Enterprise Systems and provides information security materials. People can register for the *Enterprise Strategies* newsletter at the site and search its archives as well as other information security resources.

http://www.gocsi.com/
This is the home page for the Computer Security Institute. According to the web site, "Computer Security Institute serves the needs of Information Security Professionals through membership, educational events, security surveys and awareness tools. Joining CSI provides you with high quality CSI publications, discounts on CSI conferences, access to on-line archives, career development, networking opportunities and more. CSI publishes the annual CSI/FBI Computer Crime & Security Survey, which attracts widespread media attention, and holds an annual Security Survey Roadshow in various cities. CSI Awareness offers products and training to help improve awareness that includes Frontline end user awareness newsletter, World Security Challenge web-based awareness training, awareness peer groups and more. Private training from CSI is also available for organizations."

http://h30240.www3.hp.com/courses/overview.jsp?courseId=13335&courseSessionId=6367&webPageId=1000010&hhopsession.id=d945a4712fe1df09744b78eaa492&hhopsession.id=d945a4712fe1df09744b78eaa492
This link takes you to an online training course in information security called "Security Boot Camp." The training, offered free of charge by Hewlett-Packard (HP), provides useful information to people new to information security. The materials offer useful ideas for when an organization needs to communicate the information security plan to everyone in the organization. The online HP courses can be accessed at http://h30240.www3.hp.com/index.jsp?hhopsession.id=3ed8ba66e8c2c4936b2c8a238dfe

http://www.isecom.org/osstmm/
According to the web site: "The Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing security tests and metrics. The OSSTMM test cases are divided into five channels (sections) which collectively test: information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases. The OSSTMM focuses on the technical details of exactly which items need to be tested, what to do before, during, and after a security test, and how to measure the results. New tests for international best practices, laws, regulations, and ethical concerns are regularly added and updated." This is an important site for anyone interested in OSSTMM. The web site is operated by the Institute for Security and Open Methodologies.

http://www.iwar.org.uk/ecoespionage/resources/security-guide/Contents.htm#Shortcut
This is a listing of resources provided by the Information Warfare Site (IWS), "an online resource that aims to stimulate debate about a range of subjects from information security to information operations and e-commerce. It is the aim of the site to develop a special emphasis on offensive and defensive information operations. IWS first went online in December 1999. Since its launch it has undergone a complete redesign and many key texts have been added." The materials would be of interest to information security personnel. It has an extended discussion of counterintelligence.

http://www.oissg.org/component/option,com_frontpage/Itemid,1/
This is the web site for Open Information System Security Group. According to the web site, "OISSG is a not-for-profit organization. Our vision is to spread information security awareness by hosting an environment where security enthusiasts from all over the globe share and build knowledge. To achieve our vision, we determine utmost professional need, allocate resources and develop, deliver, and promote programs that add value to the information security community." Of primary interest at the site is the Information Systems Security Assessment Framework (ISSAF). "The ISSAF is OISSG's flagship project. It is an effort to develop an end-to-end framework for security assessment. The ISSAF aims to provide a single point of reference for professionals involved in security assessment; it reflects and addresses the practical issues of security assessment. The ISSAF is an evolving framework and it will be further amended and updated."

http://www.ponemon.org/index.html
"The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the

private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries." Access to the research is restricted. Membership in the Responsible Information Management Council is required to gain access to the full site.

http://www.sans.org/?portal=4803396804b714c6beb9083a113f5363
According to its web site, "The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community."

SANS provides a large collection of research documents free of charge covering a variety of information security issues. SANS also is a vendor supplying information security training and certification.

http://www.sans.org/resources/policies/
This is the site for the SANS Security Policy Project. The site provides a good overview of security policies, standards, and guidelines, and offers a variety of policy templates that may be downloaded and customized by replacing <Company Name> with the name of your organization.

http://www.staysafeonline.info/index.html
This web site is administrated by the National Cyber Security Alliance. It provides information on cyber security for individuals and small businesses. This information is designed for non-echnical users and focuses more on individual security than business security.

http://www.us-cert.gov/
This is the home page for the United States Computer Emergency Response Team (US-CERT). The web site provides a wide array of information about cyber attacks and Internet security. The materials include those for both technical and nontechnical users.

Insider Threat

http://www.polarcove.com/whitepapers/insiderthreats.htm
This link is to a white paper from Polar Cove on insider threats. The web site provides interesting data on insider threats along with some solutions. "Polar Cove is a dynamic and innovative company providing a full range of security solutions to meet your needs for secure systems development, secure application development, network security, and information security related goals. We help our customers achieve their business objectives by developing secure

solutions that encompass your ideas, business needs, key skills, and current technology partnerships."

Overseas Travel

http://www.pueblo.gsa.gov/cic_text/travel/business-overseas/travel.html
This web site is a text version of the brochure "Personal Security Guidelines for the American Business Traveler Overseas" developed by the Bureau of Diplomatic Security, Overseas Security Advisory Council.

http://www.travel.state.gov/travel/travel_1744.html
This web site is part of the U.S. Department of State and has information from the the Office of American Citizens Services and Crisis Management (ACS). This office provides services to Americans traveling or residing abroad. The site contains valuable information abut traveling and living safely abroad with sections on "Tips for Traveling Abroad" and "Living Abroad Tips."

Pandemics (Avian Influenza)

http://www.businessroundtable.org//taskforces/taskforce/document.aspx?qs=68A5BF159FC49514481138A6DBE7A7A19BB6487B96C39B1
This is a pandemic flu preparation document prepared by the Business Roundtable, an association of leading chief executive officers in the United States. The document details its recommendations for pandemic flu preparedness.

http://www.cdc.gov/business/
This section of the Centers for Disease Control and Prevention (CDC) web site provides information about avian flu. The free resources include a business planning checklist and pandemic influenza tools for businesses. The site also contains information to help organizations plan for various types of disasters.

http://www.pandemicflu.gov/index.html
This web site is the central information hub for Avian influenza information provided by the United States government. Organizations can get facts about how they should plan, along with what federal, state, and local governments are doing to prepare. The "Workplace Planning" section provides a number of tools for organizations. Some are for specific industries, but there are general Avian influenza planning documents as well.

http://www.who.int/csr/disease/avian_influenza/en/
This section of the World Health Organization's (WHO) web site is dedicated to Avian influenza. The site offers general guidance for coping with the avian flu and links to other sites on the topic. A unique feature is this site's tracking of the global outbreaks of avian flu. Visitors to the site can view an up-to-date map of the

world to see where new and old outbreaks have occurred. This global perspective is useful for international businesses.

Shelter-in-Place

http://www.epa.gov/ord/articles/shelter_in_place_qa.htm
This web site is operated by the Environmental Protection Agency and details the concept of shelter-in-place. It is an excellent resource for any organization that may need to shelter-in-place or to warn community members to do so.

Social Engineering

www.socialengineering101.com
This site offers the social engineer possibly every tool he or she ever could need, including a chat board for sharing recent successes and failures.

Terrorism

http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/
This part of the U.S. Customs and Border Protection web site is dedicated to the Customs-Trade Partnership Against Terrorism (C-TPAT). Organizations can learn what C-TPAT is, how it can help their businesses, and requirements for certification for C-TPAT. This site is a must for any organization that wants to become part of C-TPAT.

http://www.cfr.org/issue/135/?type=issue
This web site is operated by the Council on Foreign Relations and provides information about terrorists and terrorism. Organizations that are exposed to terrorism will find useful information on such topics as counterterrorism, weapons of terrorism, terrorist organizations, and terrorism and the economy.

http://www.tkb.org/Country.jsp?countryCd=US
This links the United States page of the MIPT Terrorism Knowledge Base. "The MIPT Terrorism Knowledge Base® (TKB®) is the one-stop resource for comprehensive research and analysis on global terrorist incidents, terrorism-related court cases, and terrorist groups and leaders. TKB covers the history, affiliations, locations, and tactics of terrorist groups operating across the world, with over 35 years of terrorism incident data and hundreds of group and leader profiles and trials. TKB also features interactive maps, statistical summaries, and analytical tools that can create custom graphs and tables." The Terrorism Knowledge Base provides terrorist information for a wide range of countries along with information about terrorist groups and the ability to search the data for terrorist incidents worldwide. The site is very useful for a mult-national organization trying to determine the terrorist risks facing its various locations.

VENDORS

Data Backup

Circadian Force
Provides electronic vaulting with a focus on disaster recovery and business continuity. It serves organizations across the United States. Can be found on the web at http://www.circadianforce.com/index.htm.

EMC Corporation
Considers itself one of the world leaders in products, services, and solutions for information management and storage. It has a worldwide client list and helps organizations keep their most essential digital information protected, secure, and continuously available. Can be found on the web at http://www.emc.com/about/.

Iron Mountain Incorporated (IRM)
Provides organizations with data protection, records management, and information destruction services. The company also makes available its expertise in handling complex information challenges such as regulatory compliance and litigation. Can be found on the web at http://www.ironmountain.com/index.asp.

National Records Centers Inc. (NRC)
Services include records management, document storage, digital services, document destruction, computer media rotation, and vaulting. It serves organizations throughout North and Central America and Europe. The primary focus is off-site records management and storage services. See http:// www.nationalrecordscenters .com/default.asp.

Internet and E-mail Monitoring

Cyveillance
Provides services that allow organizations to monitor online activities, including e-mail, and to protect themselves from online risks. Cyveillance uses what it calls *proactive cyber intelligence*. It can monitor what is being said about your company as well as keep an eye on employee Internet and e-mail activity. Cyveillance offers comprehensive coverage online, including chat rooms and “hidden” networks of e-mail. Can be found on the web at http://www.cyveillance.com/.

Websense, Inc.
Advertises itself as a global leader in web filtering and desktop security software. Its Internet filtering is flexible and has integrated policy enforcement. Can be found on the web at http://www.websense.com/global/en/.

Mass Notification

3n (National Notification Network)
A leading provider of mass notification for corporations, schools, nonprofits, and government agencies. Its primary service is InstCom™, a suite of products that allows for rapid communication in emergency or urgent situations. Can be found on the web at http://www.3nonline.com/index.php.

Simulations for Training and Exercises

Crisis Simulations International
Provides real-time interactive simulations for corporations and government agencies. These realistic scenarios offer a variety of real-life situations designed to test an organization's crisis, business continuity, and emergency management skills. Can be found on the web at http://www.crisissimulations.com/index.html.

Security

Polar Cove
Provides a full range of security solutions including network security, secure application development, secure system development, and information security-related goals. Polar Cove creates a solution that meets the needs of its clients. Can be found on the web at http://www.polarcove.com/index.htm.

Redkey International
Provides specialized security risk management services. Redkey's risk management focus helps its clients maintain business continuity. Can be found on the web at http://www.redkeyinternational.com/aboutus.html.

DOCUMENT APPENDIX

SECURITY SELF-ASSESSMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS

Marianne Swanson

INTRODUCTION

A self-assessment conducted on a system (major application or general support system) or multiple self-assessments conducted for a group of interconnected systems (internal or external to the agency) is one method used to measure information technology (IT) security assurance. IT security assurance is the degree of confidence one has that the managerial, technical and operational security measures work as intended to protect the system and the information it processes. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Agencies must plan for security, ensure that the appropriate officials are assigned security responsibility, and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

An important element of ensuring an organizations' IT security health is performing routine self-assessments of the agency security program. For a self-assessment to be effective, a risk assessment should be conducted in conjunction with or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

There are many methods and tools for agency officials to help determine the current status of their security programs relative to existing policy. Ideally many of these methods and tools would be implemented on an ongoing basis to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement. This document provides a method to evaluate the security of unclassified systems or groups of systems; it guides the reader in performing an IT security self-assessment. Additionally, the document provides guidance on utilizing the results of the system self-assessment to ascertain the status of the agency-wide security program. The results are obtained in a form that can readily be used to determine which of the five levels specified in the Federal IT Security Assessment Framework the agency has achieved for each topic area covered in the questionnaire. For example, the group of systems under review may have reached level 4 (Tested and Evaluated Procedures and Controls) in the topic area of physical and environmental protection, but only level 3 (Implemented Procedures and Controls) in the area of logical access controls.

Self-Assessments

This self-assessment guide utilizes an extensive questionnaire (Appendix A) containing specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be measured. The questionnaire can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. This guide does not establish new security requirements. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. However the guide is not intended to be a comprehensive list of control objectives and related techniques. The guide should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, specific technical controls, such as those related to individual technologies or vendors, are not specifically provided due to their volume and dynamic nature. It should also be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately.

The goal of this document is to provide a standardized approach to assessing a system. This document strives to blend the control objectives found in the many requirement and guidance documents. To assist the reader, a reference source is listed after each control objective question listed in the questionnaire. Specific attention was made to the control activities found in the General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM). FISCAM is the document GAO auditors and agency inspector generals use when auditing an agency. When FISCAM is referenced in the questionnaire, the major category initials along with the control activity number are provided, e.g., *FISCAM SP-3.1*. The cross mapping of the two documents will form a road map between the control objectives and techniques the audit community assess and the control objectives and techniques IT security program managers and program officials need to assess. The mapping provides a common point of reference for individuals fulfilling differing roles in the assessment process. The mapping ensures that both parties are reviewing the same types of controls.

The questionnaire may be used to assess the status of security controls for a system, an interconnected group of systems, or agency-wide. These systems include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all security controls and all interconnected system dependencies provides a metric of the IT security conditions of an agency. By using the procedures outlined in Chapter 4, the results of the assessment can be used as input on the status of an agency's IT security program.

Federal IT Security Assessment Framework

The Federal IT Security Assessment Framework issued by the federal Chief Information Officer Council in November 2000 provides a tool that agencies can use to routinely evaluate the status of their IT security programs. The document established the groundwork for standardizing on five levels of security effectiveness and measurements that agencies could use to determine which of the five levels are met. By utilizing the Framework levels, an agency can prioritize agency efforts as well as use the document over time to evaluate progress. The NIST Self-Assessment Guide builds on the Framework by providing questions on specific areas of control, such as those pertaining to access and service continuity, and a means of categorizing evaluation results in the same manner as the Framework. See Appendix C for a copy of the Framework.

Audience

The control objectives and techniques presented are generic and can be applied to organizations in private and public sectors. This document can be used by all levels of management and by those individuals responsible for IT security at the system level and organization level. Additionally, internal and external auditors may use the questionnaire to guide their review of the IT security of systems. To perform the examination and testing required to complete the questionnaire, the assessor must be familiar with and able to apply a core knowledge set of IT security basics needed to protect information and systems. In some cases, especially in the area of examining and testing technical controls, assessors with specialized technical expertise will be needed to ensure that the questionnaire's answers are reliable.

Structure of this Document

Chapter 1 introduces the document and explains IT security assessments and the relationship to other documents. Chapter 2 provides a method for determining the system boundaries and criticality of the data. Chapter 3 describes the questionnaire. Chapter 4 provides guidance on using the completed system questionnaire(s) as input into obtaining an assessment of an agency-wide IT security program. Appendix A contains the questionnaire. Appendix B lists the documents used in compiling the assessment control objective questions. Appendix C contains a copy of the *Federal IT Security Assessment Framework*. Appendix D lists references used in developing this document.

SYSTEM ANALYSIS

The questionnaire is a tool for completing an internal assessment of the controls in place for a major application or a general support system. The security of every system or group of interconnected system(s) must be described in a security plan. The system may consist of a major application or be part of a general support system. The definition of major application and general support system are contained in Appendix C. Before the questionnaire can be used effectively, a determination must be made as to the boundaries of the system and the sensitivity and criticality of the information stored within, processed by, or transmitted by the system(s). A completed general support system or major application security plan, which is required under OMB Circular A-130, Appendix III, should describe the boundaries of the system and the criticality level of the data. If a plan has not been prepared for the system, the completion of this self-assessment will aid in developing the system security plan. Many of the control objectives addressed in the assessment are to be described in the system security plan. The following two sections, Section 2.1 and Section 2.2, contain excerpts from NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, and will assist the reader in determining the physical and logical boundaries of the system and the criticality of the information.

System Boundaries

Defining the scope of the assessment requires an analysis of system boundaries and organizational responsibilities. Networked systems make the boundaries much harder to define. Many organizations have distributed client-server architectures where servers and workstations communicate through networks. Those same networks are connected to the Internet. A system, as defined in NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems,* is identified by defining boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a system security plan and a security evaluation whenever a major modification to the system occurs. Each element of the system must[1]:

- Be under the **same** direct management control;
- Have the **same** function or mission objective;
- Have essentially the **same** operating characteristics and security needs; and
- Reside in the **same** general operating environment.

All components of a system need not be physically connected (e.g., [1] a group of stand-alone personal computers (PCs) in an office; [2] a group of PCs placed in employees' homes under defined telecommuting program rules; [3] a group of portable PCs provided to employees who require mobile computing capability to perform their jobs; and [4] a system with multiple identical configurations that are installed in locations with the same environmental and physical controls).

An important element of the assessment will be determining the effectiveness of the boundary controls when the system is part of a network. The boundary controls must protect the defined system or group of systems from unauthorized intrusions. If such boundary controls are not effective, then the security of the systems under review will depend on the security of the other systems connected to it. In the absence of effective boundary controls, the assessor should determine and document the adequacy of controls related to each system that is connected to the system under review.

Sensitivity Assessment

Effective use of the questionnaire presumes a comprehensive understanding of the value of the systems and information being assessed. Value can be expressed in terms of the degree of sensitivity or criticality of the systems and information relative to each of the five protection categories in section 3534(a)(1)(A) of the Government Information Security Reform provisions of the National Defense Authorization Act of 2000, i.e., integrity, confidentiality, availability, authenticity, and non-repudiation. The addition of authenticity and non-repudiation as protection categories within the Reform Act was to stress the need for these assurances as the government progresses towards a paperless workplace. There are differing opinions on what constitutes protection categories, for continuity within several NIST Special Publication 800 documents; authenticity, non-repudiation, and accountability are associated with the integrity of the information.

- ***Confidentiality***—The information requires protection from unauthorized disclosure.
- ***Integrity***—The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
    - *Authenticity*—A third party must be able to verify that the content of a message has not been changed in transit.
    - *Non-repudiation*—The origin or the receipt of a specific message must be verifiable by a third party.
    - *Accountability*—A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- ***Availability***—The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

When determining the value, consider any laws, regulations, or policies that establish specific requirements for integrity, confidentiality, authenticity, availability, and non-repudiation of data and information in the system. Examples might include Presidential Decision Directive 63, the Privacy Act, or a specific statute or regulation concerning the information processed (e.g., tax or census information).

Consider the information processed by the system and the need for protective measures. Relate the information processed to each of the three basic protection requirements above (**confidentiality**, **integrity**, and **availability**). In addition, it is helpful to categorize the system or group of systems by sensitivity level. Three examples of such categories for sensitive unclassified information are described below:

- *High*—Extremely grave injury accrues to U.S. interests if the information is compromised; could cause loss of life, imprisonment, major financial loss, or require legal action for correction
- *Medium*—Serious injury accrues to U.S. interests if the information is compromised; could cause significant financial loss or require legal action for correction
- *Low*—Injury accrues to U.S. interests if the information is compromised; would cause only minor financial loss or require only administrative action for correction

For example, a system and its information may require a high degree of integrity and availability, yet have no need for confidentiality.

Many agencies have developed their own methods of making these determinations. Regardless of the method used, the system owner/program official is responsible for determining the sensitivity of the system and information. The sensitivity should be considered as each control objective question in the questionnaire is answered. When a determination is made to either provide more rigid controls than are addressed by the questionnaire or not to implement the control either temporarily or permanently, there is a risk based decision field in the questionnaire that can be checked to indicate that a determination was made. The determination for lesser or more stringent protection should be made due to either the sensitivity of the data and operations affected or because there are compensating controls that lessen the need for this particular control technique. It should be noted in the comments section of the questionnaire that the system security plan contains supporting documentation as to why the specific control has or has not been implemented.

QUESTIONNAIRE STRUCTURE

The self-assessment questionnaire contains three sections: cover sheet, questions, and notes. The questionnaire begins with a cover sheet requiring descriptive information about the major application, general support system, or group of interconnected systems being assessed. The questionnaire provides a hierarchical approach to assessing a system by containing critical elements and subordinate questions. The critical element level should be determined based on the answers to the subordinate questions. The critical elements are derived primarily from OMB Circular A-130. The subordinate questions address the control objectives and techniques that can be implemented to meet the critical elements. Assessors will need to carefully review the levels of subordinate control objectives and techniques in order to determine what level has been reached for the related critical element. The control objectives were obtained from the list of source documents located in Appendix B. There is flexibility in implementing the control objectives and techniques. It is feasible that not all control objectives and techniques may be needed to achieve the critical element.

The questionnaire section may be customized by the organization. An organization can add questions, require more descriptive information, and even pre-mark certain questions if applicable. For example, many agencies may have personnel security procedures that apply to all systems within the agency. The level 1 and level 2 columns in the questionnaire can be pre-marked to reflect the standard personnel procedures in place. Additional columns may be added to reflect the status of the control, i.e., planned action date, non-applicable, or location of documentation. The questionnaire should not have questions removed or questions modified to reduce the effectiveness of the control.

After each question, there is a comment field and an initial field. The comment field can be used to note the reference to supporting documentation that is attached to the questionnaire or is obtainable for that question. The initial field can be used when a risk based decision is made concerning not to implement a control or if the control is not applicable for the system. At the end of each set of questions, there is an area provided for notes. This area may be used for denoting where in a system security plan specific sections should be modified. It can be used to document the justification as to why a control objective is not being implemented fully or why it is overly rigorous. The note section may be a good place to mark where follow-up is needed or additional testing, such as penetration testing or product evaluations, needs to be initiated. Additionally, the section may reference supporting documentation on how the control objectives and techniques were tested and a summary of findings.

Questionnaire Cover Sheet

This section provides instruction on completing the questionnaire cover sheet, standardizing on how the completed evaluation should be marked, how systems are titled, and labeling the criticality of the system.

Questionnaire Control

All completed questionnaires should be marked, handled, and controlled at the level of sensitivity determined by organizational policy. It should be noted that the information contained in a completed questionnaire could easily depict where the system or group of systems is most vulnerable.

System Identification

The cover page of the questionnaire begins with the name and title of the system to be evaluated. As explained in NIST Special Publication 800-18, each major application or general support system should be assigned a unique name/identifier.

Assigning a unique identifier to each system helps to ensure that appropriate security requirements are met based on the unique requirements for the system, and that allocated resources are appropriately applied. Further, the use of unique system identifiers is integral to the IT system investment models and analyses established under the requirements of the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act). The identifiers are required by OMB Circular A-11 and used in the annual OMB budget submissions of the Exhibit 53 and 300. In light of OMB policies concerning capital planning and investment control, the unique name/identifier should remain the same throughout the life of the system to allow the organization to track completion of security requirements over time. Please see OMB Circular A-11, Section 53.7 for additional information on assigning unique identifiers. If no unique name/identifier has been assigned or is not known, contact the information resource management office for assistance.

In many cases the major application or general support system will contain interconnected systems. The connected systems should be listed and once the assessment is complete, a determination should be made and noted on the cover sheet as to whether the boundary controls are effective. The boundary controls should be part of the assessment. If the boundary controls are not adequate, the connected systems should be assessed as well.

The line below the System Name and Title requires the assessor to mark the system category (General Support or Major Application). If an agency has additional system types or system categories, i.e., mission critical or non-mission critical, the cover sheet should be customized to include them.

Purpose and Assessor Information

The purpose and objectives of the assessment should be identified. For example, the assessment is intended to gain a high-level indication of system security in preparation for a more detailed review or the assessment is intended to be a thorough and reliable evaluation for purposes of developing an action plan. The name, title, and organization of the individuals who perform the assessment should be listed. The organization should customize the cover page accordingly.

The start date and completion date of the evaluation should be listed. The length of time required to complete an evaluation will vary. The time and resources needed to complete the assessment will vary depending on the size and complexity of the system, accessibility of system and user data, and how much information is readily available for the assessors to evaluate. For example, if a system has undergone extensive testing, certification, and documentation, the self-assessment is easy to use and serves as a baseline for future evaluations. If the system has undergone very limited amounts of testing and has poor documentation, completing the questionnaire will require more time.

Criticality of Information

The level of sensitivity of information as determined by the program official or system owner should be documented using the table on the questionnaire cover sheet. If an organization has designed their own method of determining system criticality or sensitivity, the table should be replaced with the organization's criticality or sensitivity categories. The premise behind formulating the level of sensitivity is that systems supporting higher risk operations would be expected to have more stringent controls than those that support lower risk operations.

Questions

The questions are separated into three major control areas: 1) management controls, 2) operational controls, and 3) technical controls. The division of control areas in this manner complements three other NIST Special Publications: NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook* (Handbook), NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Principles and Practices), and NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems* (Planning Guide). All three documents should be referenced for further information. The Handbook should be used to obtain additional detail for any of the questions (control objectives) listed in the questionnaire. The Principles and Practices document should be used as a reference to describe the security controls. The Planning Guide formed the basis for the questions listed in the questionnaire. The documents can be obtained from the NIST Computer Security Resource Center web site at the URL: http://csrc.nist.gov.

The questions portion of this document easily maps to the three NIST documents described above since the chapters in all three documents are organized by the same control areas, i.e., management, operational, and technical.

Within each of the three control areas, there are a number of topics; for example, personnel security, contingency planning, and incident response are topics found under the operational control area. There are a total of 17 topics contained in the questionnaire; each topic contains critical elements and supporting security control objectives and techniques (questions) about the system. The critical elements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The control objectives and techniques support the critical elements. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

Each control objective and technique may or may not be implemented depending on the system and the risk associated with the system. Under each control objective and technique question, one or more of the source documents is referenced. The reference points to the specific control activity in the GAO FISCAM document or to the title of any of the other documents listed in Appendix B, Source of Control Criteria.

In order to measure the progress of effectively implementing the needed security control, five levels of effectiveness are provided for each answer to the security control question:

- Level 1 – control objective documented in a security policy
- Level 2 – security controls documented as procedures
- Level 3 – procedures have been implemented
- Level 4 – procedures and security controls are tested and reviewed
- Level 5 – procedures and security controls are fully integrated into a comprehensive program.

The method for answering the questions can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. The review, for example, should consist of testing the access control methods in place by performing a penetration test; examining system documentation such as software change requests forms, test plans, and approvals; and examining security logs and audit trails. Supporting documentation describing what has been tested and the results of the tests add value to the assessment and will make the next review of the system easier.

Once the checklist, including all references, is completed for the first time, future assessments of the system will require considerably less effort. The completed questionnaire would establish a baseline. If this year's assessment indicates that most of the controls in place are at level 2 or level 3, then that would be the starting point for the next evaluation. More time can be spent identifying ways to increase the level of effectiveness instead of having to gather all the initial information again. Use the comment section to list whether there is supporting documentation and the notes section for any lengthy explanations.

The audit techniques to test the implementation or effectiveness of each control objective and technique are beyond the scope of this document. The GAO FISCAM document provides audit techniques that can be used to test the control objectives.

When answering the questions about whether a specific control objective has been met, consider the sensitivity of the system. The questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control. There may be certain situations where management will grant a waiver either because compensating controls exists or because the benefits of operating without the control (at least temporarily) outweigh the risk of waiting for full control implementation. Alternatively, there may be times when management implements more stringent controls than generally applied elsewhere. When the risk-based decision field is checked, note the reason in the comment field of the questionnaire and have management review and initial the decision. Additionally, the system security plan for the system should contain supporting documentation as to why the control has or has not been implemented.

The assessor must read each control objective and technique question and determine in partnership with the system owner and those responsible for administering the system, whether the system's sensitivity level warrants the implementation of the control stated in the question. If the control is applicable, check whether there are documented policies (level 1), procedures for implementing the control (level 2), the control has been implemented (level 3), the control has been tested and if found ineffective, remedied (level 4), and whether the control is part of an agency's organizational culture (level 5). The shaded fields in the questionnaire do not require a check mark. The five levels describing the state of the control objective provide a picture of each operational control; however, how well each one of these controls is met is subjective. Criteria have been established for each of the five levels that should be applied when determining whether the control objective has fully reached one or more of the five levels. The criteria are contained in Appendix C, *Federal IT Security Assessment Framework*.

Based on the responses to the control objectives and techniques and in partnership with the system owner and those responsible for system administration, the assessor should conclude the level of the related critical element. The conclusion should consider the relative importance of each subordinate objective/technique to achieving the critical element and the rigor with which the technique is implemented, enforced, and tested.

Applicability of Control Objectives

As stated above, the critical elements are required to be implemented; the control objectives and techniques, however, tend to be more detailed and leave room for reasonable subjective decisions. If the control does not reasonably apply to the system, then a "non-applicable" or "N/A" can be entered next to the question.

The control objectives and techniques in the questionnaire are geared for a system or group of connected systems. It is possible to use the questionnaire for a program review at an organizational level for ascertaining if the organization has policy and procedures in place (level 1 or level 2). However, to ensure all systems have implemented, tested and fully integrated the controls (level 3, level 4, and level 5), the assessment questionnaire must be applied to each individual or interconnected group of systems. Chapter 4 describes how the results of the assessment can be used as input into an IT security program review.

The policy and procedures for a control objective and technique can be found at the Department level, agency level, agency component level, or application level. To effectively assess a system, ensure that the control objectives being assessed are at the applicable level. For example, if the system being reviewed has stringent authentication procedures, the authentication procedures for the system should be assessed, instead of the agency-wide minimum authentication procedures found in the agency IT security manual.

If a topic area is documented at a high level in policy, the level 1 box should be checked in the questionnaire. If there are additional low level policies for the system, describe the policies in the comment section of the questionnaire. If a specific control is described in detail in procedures, and implemented, the level 2 and level 3 boxes should be checked in the questionnaire. Testing and reviewing controls are an essential part of securing a system. For each specific control, check whether it has been tested and/or reviewed when a significant change occurred. The goal is to have all levels checked for each control. A conceptual sample of completing the questionnaire is contained in Appendix C. The conceptual sample has evolved into the questionnaire and differs slightly, i.e., there is now a comment and initial field.

UTILIZING THE COMPLETED QUESTIONNAIRE

The questionnaire can be used for two purposes. First it can be used by agency managers who know their agency's systems and security controls to quickly gain a general understanding of where security for a system, group of systems, or the entire agency needs improvement. Second, it can be used as a guide for thoroughly evaluating the status of security for a system. The results of such thorough reviews provide a much more reliable measure of security effectiveness and may be used to 1) fulfill reporting requirements; 2) prepare for audits; and 3) identify resource needs.

Questionnaire Analysis

Because this is a self-assessment, ideally the individuals assessing the system are the owners of the system or responsible for operating or administering the system. The same individuals who completed the assessment can conduct the analysis of the completed questionnaire. By being familiar with the system, the supporting documentation, and the results of the assessment, the next step that the assessor takes is an analysis, which summarizes the findings. A centralized group, such as an agency's Information System Security Program Office, can also conduct the analysis as long as the supporting documentation is sufficient. The results of the analysis should be placed in an action plan, and the system security plan should be created or updated to reflect each control objective and technique decision.

Action Plans

How the critical element is to be implemented, i.e., specific procedures written, equipment installed and tested, and personnel trained, should be documented in an action plan. The action plan must contain projected dates, an allocation of resources, and follow-up reviews to ensure that remedial actions have been effective. Routine reports should be submitted to senior management on weaknesses identified, the status of the action plans, and the resources needed.

Agency IT Security Program Reports

Over the years, agencies have been asked to report on the status of their IT security program. The reporting requests vary in how much detail is required and in the type of information that should be reported. The completed self-assessment questionnaires are a useful resource for compiling agency reports. Below are sample topics that should be considered in an agency-wide security program report:

- Security Program Management
- Management Controls
- Operational Controls
- Technical Controls
- Planned Activities

Security Program Management

An agency's IT security program report needs to address programmatic issues such as:

- an established agency-wide security management structure,
- a documented up-to-date IT security program plan or policy (*The assessment results for level 1 provides input.*)
    - an agency-developed risk management and mitigation plan,
    - an agency-wide incident response capability,
    - an established certification and accreditation policy,
    - an agency-wide anti-virus infrastructure in place and operational at all agency facilities,
    - information security training and awareness programs established and available to all agency employees,
    - roles and relationships clearly defined and established between the agency and bureau levels of information security program management,
- an understanding of the importance of protecting mission critical information assets,
- the integration of security into the capital planning process,
- methods used to ensure that security is an integral part of the enterprise architecture (*The assessment results for the Life Cycle topic area provides input.*),
- the total security cost from this year's budget request and a breakdown of security costs by each major operating division, and
- descriptions of agency-wide guidance issued in the past year.

Management Controls, Operational Controls, and Technical Controls

The results of the completed questionnaires' 17 control topic areas can be used to summarize an agency's implementation of the management, operational, and technical controls. For the report to project an accurate picture, the results must be summarized by system type, not totaled into an overall agency grade level. For example, ten systems were assessed using the questionnaire. Five of the ten systems assessed were major applications; the other five were general support systems. The summary would separate the systems into general support systems and major applications.

By further separating them into groups according to criticality, the report stresses which systems and which control objectives require more attention based on sensitivity and criticality. Not all systems require the same level of protection; the report should reflect that diversity. The use of percentages for describing compliance (i.e., 50 percent of the major applications and 25 percent of general support systems that are high in criticality have complete and current system security plans within the past three years) can be used as long as there is a distinct division provided between the types of systems being reported.

Additionally all or a sampling of the completed questionnaires can be analyzed to determine which controls if implemented would impact the most systems. For example, if viruses frequently plague systems, a stricter firewall policy that prevents attached files in E-mail may be a solution. Also, systemic problems should be culled out. If an agency sees an influx of poor password management controls in the questionnaire results, then possibly password checkers should be used, awareness material issued, and password- aging software installed.

The report should conclude with a summary of planned IT security initiatives. The summary should include goals, actions needed to meet the goals, projected resources, and anticipated dates of completion.

APPENDIX A

System Questionnaire

System Name, Title, and Unique Identifier: ______________________________

Major Application _____________ or General Support System _____________

Name of Assessors: ____

____

____

Date of Evaluation: ______________________________

List of Connected Systems:

Name of System	Are boundary controls effective?	Planned action if not effective
1.		
2.		
3.		

Criticality System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: ______________________________

____

____

Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management *OMB Circular A-130, III*								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								
1.1.3 Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*								
1.1.4 Have threat sources, both natural and manmade, been identified? *FISCAM SP-1*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? *NIST SP 800-30*[2]								
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? *NIST SP 800-30*								
1.2. Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								
1.2.1 Are final risk determinations and related management approvals documented and maintained on file? *FISCAM SP-1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.2.2 Has a mission/business impact analysis been conducted? *NIST SP 800-30*								
1.2.3. Have additional controls been identified to sufficiently mitigate identified risks? *NIST SP 800-30*								

Notes:

Review of Security Controls

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2. Review of Security Controls *OMB Circular A-130, III* *FISCAM SP-5* *NIST SP 800-18*								
2.1. Critical Element: Have the security controls of the system and interconnected systems been reviewed?								
2.1.1 Has the system and all network boundaries been subjected to periodic reviews? *FISCAM SP-5.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2.1.2 Has an independent review been performed when a significant change occurred? *OMB Circular A-130, III* *FISCAM SP-5.1* *NIST SP 800-18*								
2.1.3 Are routine self-assessments conducted? *NIST SP 800-18*								
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? *OMB Circular A-130, 8B3* *NIST SP 800-18*								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? *FISCAM SP 3-4* *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2.2. Critical Element: Does management ensure that corrective actions are effectively implemented?								
2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action? *FISCAM SP 5-1 and 5.2* *NIST SP 800-18*								

Notes:

Life Cycle

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
3. Life Cycle *OMB Circular A-130, III* *FISCAM CC-1.1*								
3.1. Critical Element: Has a system development life cycle methodology been developed?								
Initiation Phase								
3.1.1. Is the sensitivity of the system determined? *OMB Circular A-130, III* *FISCAM AC-1.1 & 1.2* *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.2. Does the business case document the resources required for adequately securing the system? *Clinger-Cohen*								
3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed? *Clinger-Cohen*								
3.1.4 Are authorization for software modifications documented and maintained? *FISCAM CC-1.2.*								
3.1.5 Does the budget request include the security resources required for the system? *GISRA*								
Development/Acquisition Phase								
3.1.6 During the system design, are security requirements identified? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.7 Was an initial risk assessment performed to determine security requirements? *NIST SP 800-30*								
3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk? *NIST SP 800-18*								
3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency? *OMB Circular A-130, 8B3*								
3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.11 Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures? *NIST SP 800-18*								
3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/ vulnerabilities are identified and as new technologies are implemented? *NIST SP 800-18*								
Implementation Phase								
3.2. Critical Element: Are changes controlled as programs progress through testing to final approval?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.1 Are design reviews and system tests run prior to placing the system in production? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.2 Are the test results documented? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.3 Is certification testing of security controls conducted and documented? *NIST SP 800-18*								
3.2.4 If security controls were added since development, has the system documentation been modified to include them? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? *NIST SP 800-18*								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? *NIST SP 800-18*								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? *NIST SP 800-18*								
3.2.10 Is the system security plan kept current? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? *FISCAM AC-3.4* *NIST SP 800-18*								
3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized? *NIST SP 800-18*								

Notes:

Authorize Processing (Certification & Accreditation)

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
Authorize Processing (Certification & Accreditation) *OMB Circular A-130, III* *FIPS 102*								
4.1.Critical Element: Has the system been certified/ recertified and authorized to process (accredited)?								
4.1.1 Has a technical and/ or security evaluation been completed or conducted when a significant change occurred? *NIST SP 800-18*								
4.1.2 Has a risk assessment been conducted when a significant change occurred? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
4.1.3 Have Rules of Behavior been established and signed by users? *NIST SP 800-18*								
4.1.4 Has a contingency plan been developed and tested? *NIST SP 800-18*								
4.1.5 Has a system security plan been developed, updated, and reviewed? *NIST SP 800-18*								
4.1.6 Are in-place controls operating as intended? *NIST SP 800-18*								
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? *NIST 800-18*								
4.2. Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies? *NIST SP 800-18*								

Notes:

System Security Plan

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5. System security plan *OMB Circular A-130, III* *NIST SP 800-18* *FISCAM SP-2.1*								
5.1. Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?								
5.1.1 Is the system security plan approved by key affected parties and management? *FISCAM SP-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? *NIST SP 800-18*								
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? *OMB Circular A-130, III* *NIST SP 800-18*								
5.2. Critical Element: Is the plan kept current?								
5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? *FISCAM SP-2.1* *NIST SP 800-18*								

Notes:

OPERATIONAL CONTROLS

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Personal Security *OMB Circular A-130, III*								
6.1.Critical Element: Are duties separated to ensure least privilege and individual accountability?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.1 Are all positions reviewed for sensitivity level? *FISCAM SD-1.2* *NIST SP 800-18*								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? *FISCAM SD-1.2*								
6.1.3 Are sensitive functions divided among different individuals? *OMB Circular A-130, III* *FISCAM SD-1* *NIST SP 800-18*								
6.1.4 Are distinct systems support functions performed by different individuals? *FISCAM SD-1.1*								
6.1.5 Are mechanisms in place for holding users responsible for their actions? *OMB Circular A-130, III* *FISCAM SD-2 & 3.2*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? *FISCAM SD-1.1* *FISCAM SP-4.1*								
6.1.7 Are hiring, transfer, and termination procedures established? *FISCAM SP-4.1* *NIST SP 800-18*								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? *FISCAM SP-4.1* *NIST 800-18*								
6.2. Critical Element: **Is appropriate background screening for assigned positions completed prior to granting access?**								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? *OMB Circular A-130, III* *FISCAM SP-4.1*								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? *FISCAM SP-4.1*								
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? *OMB Circular A-130, III*								
6.2.4 Are there conditions for allowing system access prior to completion of screening? *FISCAM AC-2.2* *NIST SP 800-18*								

Notes:

Physical and Environmental Protection

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection								
Physical Access Control								
7.1. Critical Element: **Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?**								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? *FISCAM AC-3* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities? *FISCAM AC-3.1*								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? *FISCAM AC-3.1*								
7.1.4 Are keys or other access devices needed to enter the computer room and tape/ media library? *FISCAM AC-3.1*								
7.1.5 Are unused keys or other entry devices secured? *FISCAM AC-3.1*								
7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? *FISCAM AC-3.1*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.7 Are visitors to sensitive areas signed in and escorted? *FISCAM AC-3.1*								
7.1.8 Are entry codes changed periodically? *FISCAM AC-3.1*								
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? *FISCAM AC-4*								
7.1.10 Is suspicious access activity investigated and appropriate action taken? *FISCAM AC-4.3*								
7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? *FISCAM AC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Fire Safety Factors								
7.1.12 Are appropriate fire suppression and prevention devices installed and working? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically? *NIST SP 800-18*								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained? *NIST SP 800-18*								
7.1.15 Is there a redundant air-cooling system? *FISCAM SC-2.2*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.17 Are building plumbing lines known and do not endanger system? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.18 Has an uninterruptible power supply or backup generator been provided? *FISCAM SC-2.2*								
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? *FISCAM SC-2.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Interception of Data								
7.2. Critical Element: Is data protected from interception?								
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? *NIST SP 800-18*								
7.2.2 Is physical access to data transmission lines controlled? *NIST SP 800-18*								
Mobile and Portable Systems								
7.3. Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems? *NIST SP 800-14*								
7.3.2 Are portable systems stored securely? *NIST SP 800-14*								

Notes:

Production, Input/Output Controls

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
Production, Input/ Output Controls								
8.1. Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice? *NIST SP 800-18*								
8.2. Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media? *NIST SP 800-18*								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? *NIST SP 800-18*								
8.2.4 Are controls in place for transporting or mailing media or printed output? *NIST SP 800-18*								
8.2.5 Is there internal/external labeling for sensitivity? *NIST SP 800-18*								
8.2.6 Is there external labeling with special handling instructions? *NIST SP 800-18*								
8.2.7 Are audit trails kept for inventory management? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.8 Is media sanitized for reuse? *FISCAM AC-3.4* *NIST SP 800-18*								
8.2.9 Is damaged media stored and/or destroyed? *NIST SP 800-18*								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed? *NIST SP 800-18*								

Notes:

Contingency Planning

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
Contingency Planning *OMB Circular A-130, III*								
9.1. Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented? *FISCAM SC-1.1 & 3.1* *N/STSP 800-18*								
9-1.2 Are resources supporting critical operations identified? *FISCAM SC-1.2*								

(*Continued*)

Specific Control Objectives	L.1	L.2	L.3	L.4	L.5	Risk Based		
and Techniques	Policy	Procedures	Implemented	Tested	Integrated	Decision Made	Comments	Initials
9.1.3 Have processing priorities been established and approved by management? *FISCAM SC-1.3*								
9.2. Critical Element: Has a comprehensive contingency plan been developed and documented?								
9.2.1 Is the plan approved by key affected parties? *FISCAM SC-3.1*								
9.2.2 Are responsibilities for recovery assigned? *FISCAM SC-3.1*								
9.2.3 Are there detailed instructions for restoring operations? *FISCAM SC-3.1*								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? *FISCAM SC-3.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.2.5 Is the location of stored backups identified? *NIST SP 800-18*								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? *FISCAM SC-2.1*								
9.2.7 Is system and application documentation maintained at the off-site location? *FISCAM SC-2.1*								
9.2.8 Are all system defaults reset after being restored from a backup? *FISCAM SC-3.1*								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? *FISCAM SC-2.1*								

(*Continued*)

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
9.2.10 Has the contingency plan been distributed to all appropriate personnel? *FISCAM SC-3.1*								
9.3. Critical Element: Are tested contingency/disaster recovery plans in place?								
9.3.1 Is an up-to-date copy of the plan stored securely off-site? *FISCAM SC-3.1*								
9.3.2 Are employees trained in their roles and responsibilities? *FISCAM SC-2.3* *NIST SP 800-18*								
9.3.3 Is the plan periodically tested and readjusted as appropriate? *FISCAM SC-3.1* *NIST SP 800-18*								

Notes:

Hardware and System Software Maintenance

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
Hardware and System Software Maintenance *OMB Circular A-130, III*								
10.1. Critical Element: Is access limited to system software and hardware?								
10.1.1 Are restrictions in place on who performs maintenance and repair activities? *OMB Circular A-130, III* *FISCAM SS-3.1* *NIST SP 800-18*								
10.1.2 Is access to all program libraries restricted and controlled? *FISCAM CC-3.2 & 3.3*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? *NIST SP 800-18*								
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? *FISCAM SS-1.2*								
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? *FISCAM SS-2.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2. Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control? *NIST SP 800-18*								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? *FISCAMSS-3.1, 3.2, & CC-2.1* *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.3 Are software change request forms used to document requests and related approvals? *FISCAM CC-1.2* *NIST SP 800-18*								
10.2.4 Are there detailed system specifications prepared and reviewed by management? *FISCAM CC-2.1*								
10.2.5 Is the type of test data to be used specified, i.e., live or made up? *NIST SP 800-18*								
10.2.6 Are default settings of security features set to the most restrictive mode? *PSN Security Assessment Guidelines*								
10.2.7 Are there software distribution implementation orders including effective date provided to all locations? *FISCAM CC-2.3*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.8 Is there version control? *NIST SP 800-18*								
10.2.9 Are programs labeled and inventoried? *FISCAM CC-3.1*								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? *FISCAM SS-3 2*								
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? *FISCAM CC-2.2*								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? *FISCAM SC-2.1* *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.13 Is the use of copyrighted software or shareware and personally owned software/ equipment documented? *NIST SP 800-18*								
10.3. Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? *NIST SP 800-18*								
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? *NIST SP 800-18*								

Notes:

Data Integrity

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
Data Integrity *OMB Circular A-130, 8B3*								
11.1. Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated? *NIST SP 800-18*								
11.1.2 Are virus scans automatic? *NIST SP 800-18*								
11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? *NIST SP 800-18*								
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken? *F1SCAM SS-2.2*								
11.2.3 Are procedures in place to determine compliance with password policies? *NIST SP 800-18*								
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? *NIST SP 800-18*								
11.2.5 Are intrusion detection tools installed on the system? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? *NIST SP 800-18*								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? *NIST SP 800-18*								
11.2.8 Is penetration testing performed on the system? *NIST SP 800-18*								
11.2.9 Is message authentication used? *NIST SP 800-18*								

Notes:

Documentation

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. When answering whether there are procedures for each control objective, the question should be phrased "are there procedures for ensuring the documentation is obtained and maintained." The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
Documentation *OMB Circular A-130, 8B3*								
12.1. Critical Element: Is there sufficient documentation that explains how software/ hardware is to be used?								
12.1.1 Is there vendor-supplied documentation of purchased software? *NIST SP 800-18*								
12.1.2 Is there vendor-supplied documentation of purchased hardware? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.1.3 Is there application documentation for in-house applications? *NIST SP 800-18*								
12.1.4 Are there network diagrams and documentation on setups of routers and switches? *NIST SP 800-18*								
12.1.5 Are there software and hardware testing procedures and results? *NIST SP 800-18*								
12.1.6 Are there standard operating procedures for all the topic areas covered in this document? *NIST SP 800-18*								
12.1.7 Are there user manuals? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.1.8 Are there emergency procedures? *NIST SP 800-18*								
12.1.9 Are there backup procedures? *NIST SP 800-18*								
12.2. Critical Element: Are there formal security and operational procedures documented?								
12.2.1 Is there a system security plan? *OMB Circular A-130, III* *FISCAM SP-2.1* *NIST SP 800-18*								
12.2.2 Is there a contingency plan? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.2.3 Are there written agreements regarding how data is shared between interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
12.2.4 Are there risk assessment reports? *NIST SP 800-18*								
12.2.5 Are there certification and accreditation documents and a statement authorizing the system to process? *NIST SP 800-18*								

Notes:

Security Awareness, Training, and Education

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	**L.1 Policy**	**L.2 Procedures**	**L.3 Implemented**	**L.4 Tested**	**L.5 Integrated**	**Risk Based Decision Made**	**Comments**	**Initials**
Security Awareness, Training, and Education *OMB Circular A-130, III*								
13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?								
13.1.1 Have employees received a copy of the Rules of Behavior? *NIST SP 800-18*								
13.1.2 Are employee training and professional development documented and monitored? *FISCAM SP-4.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
13.1.3 Is there mandatory annual refresher training? *OMB Circular A-130, III*								
13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets? *NIST SP 800-18*								
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? *NIST SP 800-18*								

Notes:

Incident Response Capability

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and impact far-reaching. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Incident Response Capability *OMB Circular A-130, III* *FISCAM SP-3.4* *NIST 800-18*								
14.1. Critical Element: **Is there a capability to provide help to users when a security incident occurs in the system?**								
14.1.1 Is a formal incident response capability available? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.2 Is there a process for reporting incidents? *FISCAM SP-3.4* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.3 Are incidents monitored and tracked until resolved? *NIST SP 800-18*								
14.1.4 Are personnel trained to recognize and handle incidents? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.5 Are alerts/advisories received and responded to? *NIST SP 800-18*								
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? *NIST SP 800-18*								
14.2. Critical Element: **Is incident related information shared with appropriate organizations?**								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
14.2.2 Is incident information shared with FedCIRC[3] concerning incidents and common vulnerabilities and threats? *OMB A-130, III* *GISRA*								
14.2.3 Is incident information reported to FedCIRC, NIPC,[4] and local law enforcement when necessary? *OMB A-130, III* *GISRA*								

Notes:

TECHNICAL CONTROLS

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Identification and Authentication

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering IT system. Access control usually requires that the system be able to identify and differentiate among users. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Identification and Authentication *OMB Circular A-130, III* *FISCAM AC-2* *NIST SP 800-18*								
15.1. Critical Element: Are users individually authenticated via passwords, tokens, or other devices?								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.1 Is a current list maintained and approved of authorized users and their access? *FISCAM AC-2* *NIST SP 800-18*								
15.1.2 Are digital signatures used and conform to FIPS 186-2? *NIST SP 800-18*								
15.1.3 Are access scripts with embedded passwords prohibited? *NIST SP 800-18*								
15.1.4 Is emergency and temporary access authorized? *FISCAM AC-2.2*								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? *FISCAM AC-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.6 Are passwords changed at least every ninety days or earlier if needed? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.8 Are inactive user identifications disabled after a specified period of time? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.9 Are passwords not displayed when entered? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.10 Are there procedures in place for handling lost and compromised passwords? *FISCAM AC-3.2* *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? *NIST SP 800-18*								
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.13 Are vendor-supplied passwords replaced immediately? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? *FISCAM AC-3.2* *NIST SP 800-18*								
15.2. Critical Element: Are access controls enforcing segregation of duties?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.2.1 Does the system correlate actions to users? *OMB A-130, III* *FISCAM SD-2.1*								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? *FISCAM AC-2.1*								

Notes:

Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Logical Access Controls *OMB Circular A-130, III* *FISCAM AC-3.2* *NIST SP-800-18*								
16.1. Critical Element: **Do the logical access controls restrict users to authorized transactions and functions?**								
16.1.1 Can the security controls detect unauthorized access attempts? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? *FISCAM AC-3.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.3 Is access to security software restricted to security administrators? *FISCAM AC-3.2*								
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.5 Are inactive users' accounts monitored and removed when not needed? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.7 If encryption is used, does it meet federal standards? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? *NIST SP 800-18*								
16.1.9 Is access restricted to files at the logical view or field? *FISCAM AC-3.2*								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated? *FISCAM AC-4*								
16.2. Critical Element: Are there logical controls over network access?								
16.2.1 Has communication software been implemented to restrict access through specific terminals? *FISCAM AC-3.2*								
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? *PSN Security Assessment Guidelines*								
16.2.4 Are there controls that restrict remote access to the system? *NIST SP 800-18*								
16.2.5 Are network activity logs maintained and reviewed? *FISCAM AC-3.2*								
16.2.6 Does the network connection automatically disconnect at the end of a session? *FISCAM AC-3.2*								
16.2.7 Are trust relationships among hosts and external entities appropriately restricted? *PSN Security Assessment Guidelines*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.8 Is dial-in access monitored? *FISCAM AC-3.2*								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? *FISCAM AC-3.2*								
16.2.10 Are firewalls or secure gateways installed? *NIST SP 800-18*								
16.2.11 If firewalls are installed do they comply with firewall policy and rules? *FISCAM AC-3.2*								
16.2.12 Are guest and anonymous accounts authorized and monitored? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.13 Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished? *FISCAM AC-3.2* *NIST SP 800-18*								
16.2.14 Are sensitive data transmissions encrypted? *FISCAM AC-3.2*								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? *FISCAM AC-3.2*								
16.3. Critical Element: If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?								
16.3.1 Is a privacy policy posted on the web site? *OMB-99-18*								

Notes:

Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The following questions are organized under one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Audit Trails *OMB Circular A-130, III* *FISCAM AC-4.1* *NIST SP 800-18*								
17.1. Critical Element: Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?								
17.1.1 Does the audit trail provide a trace of user actions? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? *NIST SP 800-18*								
17.1.3 Is access to online audit logs strictly controlled? *NIST SP 800-18*								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? *NIST SP 800-18*								
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? *NIST SP 800-18*								
17.1.6 Are audit trails reviewed frequently? *NIST SP 800-18*								

(*Continued*)

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.7 Are automated tools used to review audit records in real time or near real time? *NIST SP 800-18*								
17.1.8 Is suspicious activity investigated and appropriate action taken? *FISCAM AC-4.3*								
17.1.9 Is keystroke monitoring used? If so, are users notified? *NIST SP 800-18*								

Notes:

APPENDIX B—SOURCE OF CONTROL CRITERIA

Office of Management and Budget Circular A-130, “Management of Federal Information Resources,” Section 8B3 and Appendix III, “Security of Federal Automated Information Resources.”	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987.	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995.	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996.	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, “Protecting America’s Critical Infrastructures.”	This directive specifies agency responsibilities for protecting the nation’s infrastructure, assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
OMB Memorandum 99-18, “Privacy Policies on Federal Web Sites.”	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
General Accounting Office “Federal Information System Control Audit Manual” (FISCAM).	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, “Generally Accepted Principles and Practices for Security Information Technology Systems.”	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.

(continued)

NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."	This publication details the specific controls that should be documented in a system security plan.
Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, "Government Information Security Reform" (GISRA)	The act primarily addresses the program management and evaluation aspects of security.
Office of the Manager, National Communications Systems, "Public Switched Network Security Assessment Guidelines."	The guide describes a risk assessment procedure, descriptions of a comprehensive security program, and a summary checklist.
Federal Information Processing Standards.	These documents contain mandates and/or guidance for improving the utilization and management of computers and IT systems in the Federal Government.

APPENDIX C—FEDERAL INFORMATION TECHNOLOGY SECURITY ASSESSMENT FRAMEWORK

Overview

Information and the systems that process it are among the most valuable assets of any organization. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Agencies must plan for security, and ensure that the appropriate officials are assigned security responsibility and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

The Federal Information Technology (IT) Security Assessment Framework (or Framework) provides a method for agency officials to 1) determine the current status of their security programs relative to existing policy and 2) where necessary, establish a target for improvement. It does not establish new security requirements. The Framework may be used to assess the status of security controls for a given asset or collection of assets. These assets include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs, or operational programs (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all asset security controls and all interconnected systems that the asset depends on produces a picture of both the security condition of an agency component and of the entire agency.

The Framework comprises five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement. Coupled with the NIST-prepared self-assessment questionnaire,[5] the Framework provides a vehicle for consistent and effective measurement of the security status for a given asset. The security status is measured by determining if specific security controls are documented, implemented, tested and reviewed, and incorporated into a cyclical review/improvement program, as well as whether unacceptable risks are identified and mitigated. The NIST questionnaire provides specific questions that identify the control criteria against which agency policies, procedures, and security controls can be compared. Appendix A contains a sample of the upcoming NIST Special Publication.

The Framework is divided into five levels: Level 1 of the Framework reflects that an asset has documented security policy. At level 2, the asset also has documented procedures and controls to implement the policy. Level 3 indicates that procedures and controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At level 5, the asset has procedures and controls fully integrated into a comprehensive program.

Each level represents a more complete and effective security program. OMB and the Council recognize that the security needs for the tens of thousands of Federal information systems differ. Agencies should note that testing the effectiveness of the asset and all interconnected systems that the asset depends on is essential to understanding whether risk has been properly mitigated. When an individual system does not achieve level 4, agencies should determine whether that system meets the criteria found in OMB Memorandum M00-07 (February 28, 2000) "Incorporating and Funding Security in Information Systems Investments." Agencies should seek to bring all assets to level 4 and ultimately level 5.

Integral to all security programs whether for an asset or an entire agency is a risk assessment process that includes determining the level of sensitivity of information and systems. Many agencies have developed their own methods of making these determinations. For example, the Department of Health and Human Services uses a four—track scale for confidentiality, integrity, and availability. The Department of Energy uses five groupings or "clusters" to address sensitivity.

Regardless of the method used, the asset owner is responsible for determining how sensitive the asset is, what level of risk is acceptable, and which specific controls are necessary to provide adequate security to that asset. Again, each implemented security control must be periodically tested for effectiveness. The decision to implement and the results of the testing should be documented.

Framework Description

The Federal Information Technology Security Assessment Framework (Framework) identifies five levels of IT security program effectiveness (see Figure 1). The five levels measure specific management, operational, and technical control objectives. Each of the five levels contains criteria to determine if the level is adequately implemented. For example, in level 1, all written policy should contain the purpose and scope of the policy, the individual(s) responsible for implementing the policy, and the consequences and penalties for not following the policy. The policy for an individual control must be reviewed to ascertain that the criteria for level 1 are met. Assessing the effectiveness of the individual controls, not simply their existence, is key to achieving and maintaining adequate security.

The asset owner, in partnership with those responsible for administering the information assets (which include IT systems), must determine whether the measurement criteria are being met at each level. Before making such a determination, the degree of sensitivity of information and systems must be determined by considering the requirements for confidentiality, integrity, and availability of both the information and systems—the value of information and systems is one of the major factors in risk management.

A security program may be assessed at various levels within an organization. For example, a program could be defined as an agency asset, a major application, general support system, high impact program, physical plant, mission critical system, or logically related group of systems. The Framework refers to this grouping as an asset.

The Framework describes an asset self-assessment and provides levels to guide and prioritize agency efforts as well as a basis to measure progress. In addition, the National Institute of Standards and Technology (NIST) will develop a questionnaire that gives the implementation tools for the Framework. The questionnaire will contain specific control objectives that should be applied to secure a system.

Level 1	Documented Policy
Level 2	Documented Procedures
Level 3	Implemented Procedures and Controls
Level 4	Tested and Reviewed Procedures and Controls
Level 5	Fully Integrated Procedures and Controls

Figure 1 Federal IT Security Assessment Framework

The Framework approach begins with the premise that all agency assets must meet the minimum security requirements of the Office of Management and Budget Circular A-130, "Management of Federal Resources," Appendix III, "Security of Federal Automated Information Resources" (A-130). The criteria that are outlined in the Framework and provided in detail in the questionnaire are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. It should be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately. A list of the documents that the Framework and the questionnaire draw upon is provided below.

Source of Control Criteria

Office of Management and Budget Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources."	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987.	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995.	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996.	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, "Protecting America's Critical Infrastructures."	This directive specifies agency responsibilities for protecting the nation's infrastructure, assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
Presidential Decision Directive 67, "Enduring Constitutional Government and Continuity of Government."	Relates to ensuring constitutional government, continuity of operations (COOP) planning, and continuity of government (COG) operations.

OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records."	This memorandum provides instructions to agencies on how to comply with the President's Memorandum of May 14, 1998 on "Privacy and Personal Information in Federal Records."
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites."	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Web Sites."	The purpose of this memorandum is a reminder that each agency is required by law and policy to establish clear privacy policies for its web activities and to comply with those policies.
General Accounting Office "Federal Information System Control Audit Manual" (FISCAM).	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Security Information Technology Systems."	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."	This publication details the specific controls that should be documented in a system security plan.
Federal Information Processing Standards.	This document contains legislative and executive mandates for improving the utilization and management of computers and IT systems in the Federal Government

DOCUMENTED POLICY—LEVEL 1

Description

Level 1 of the Framework includes:

- Formally documented and disseminated security policy covering agency headquarters and major components (e.g., bureaus and operating divisions). The policy may be asset specific.
- Policy that references most of the basic requirements and guidance issued from the documents listed in the Source of Control Criteria.

An asset is at level 1 if there is a formally, up-to-date documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and uses monitoring for program effectiveness. Such a policy may include major agency components, (e.g., bureaus and operating divisions) or specific assets.

A documented security policy is necessary to ensure adequate and cost effective organizational and system security controls. A sound policy delineates the security management structure and clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance. The criteria listed below should be applied when assessing the policy developed for the controls that are listed in the NIST questionnaire.

Criteria

Level 1 criteria describe the components of a security policy.

Criteria for Level 1

a. Purpose and scope. An up-to-date security policy is written that covers all major facilities and operations agency-wide or for the asset. The policy is approved by key affected parties and covers security planning, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The policy clearly identifies the purpose of the program and its scope within the organization.

b. Responsibilities. The security program comprises a security management structure with adequate authority, and expertise. IT security manager(s) are appointed at an overall level and at appropriate subordinate levels. Security responsibilities and expected behaviors are clearly defined for asset owners and users, information resources management and data processing personnel, senior management, and security administrators.

c. Compliance. General compliance and specified penalties and disciplinary actions are also identified in the policy.

DOCUMENTED PROCEDURES—LEVEL 2

Description

Level 2 of the Framework includes:

- Formal, complete, well-documented procedures for implementing policies established at level one.
- The basic requirements and guidance issued from the documents listed in the Source of Control Criteria.

An asset is at level 2 when formally documented procedures are developed that focus on implementing specific security controls. Formal procedures promote the continuity of the security program. Formal procedures also provide the foundation for a clear, accurate, and complete understanding of the program implementation. An understanding of the risks and related results should guide the strength of the control and the corresponding procedures. The procedures document the implementation of and the rigor in which the control is applied. Level 2 requires procedures for a continuing cycle of assessing risk and vulnerabilities, implementing effective security policies, and monitoring effectiveness of the security controls. Approved system security plans are in place for all assets.

Well-documented and current security procedures are necessary to ensure that adequate and cost effective security controls are implemented. The criteria listed below should be applied when assessing the quality of the procedures for controls outlined in the NIST questionnaire.

Criteria

Level 2 criteria describe the components of security procedures.

Criteria for Level 2

a. **Control areas listed and organization's position stated.** Up-to-date procedures are written that covers all major facilities and operations within the asset. The procedures are approved by key responsible parties and cover security policies, security plans, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The procedures clearly identify management's position and whether there are further guidelines or exceptions.
b. **Applicability of procedures documented.** Procedures clarify where, how, when, to, whom, and about what a particular procedure applies.
c. **Assignment of IT security responsibilities and expected behavior.** Procedures clearly define security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and data processing personnel, (3) management, and (4) security administrators.
d. **Points of contact and supplementary information provided.** Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance.

IMPLEMENTED PROCEDURES AND CONTROLS—LEVEL 3

Description

Level 3 of the Framework includes:

- Security procedures and controls that are implemented.

- Procedures that are communicated and individuals who are required to follow them.

At level 3, the IT security procedures and controls are implemented in a consistent manner and reinforced through training. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. Security controls for an asset could be implemented and not have procedures documented, but the addition of formal documented procedures at level 2 represents a significant step in the effectiveness of implementing procedures and controls at level 3. While testing the on-going effectiveness is not emphasized in level 3, some testing is needed when initially implementing controls to ensure they are operating as intended. The criteria listed below should be used to determine if the specific controls listed in the NIST questionnaire are being implemented.

Criteria

Level 3 criteria describe how an organization can ensure implementation of their security procedures.

Criteria for Level 3

a. **Owners and users are made aware of security policies and procedures.** Security policies and procedures are distributed to all affected personnel, including system/application rules and expected behaviors. Requires users to periodically acknowledge their awareness and acceptance of responsibility for security.

b. **Policies and procedures are formally adopted and technical controls installed.** Automated and other tools routinely monitor security. Established policy governs review of system logs, penetration testing, and internal/external audits.

c. **Security is managed throughout the life cycle of the system.** Security is considered in each of the life-cycle phases: initiation, development/acquisition, implementation, operation, and disposal.

d. **Procedures established for authorizing processing (certification and accreditation).** Management officials must formally authorize system operations and manage risk.

e. **Documented security position descriptions.** Skill needs and security responsibilities in job descriptions are accurately identified.

f. **Employees trained on security procedures.** An effective training and awareness program tailored for varying job functions is planned, implemented, maintained, and evaluated.

TESTED AND EVALUATED PROCEDURES AND CONTROLS—LEVEL 4

Description

Level 4 of the Framework includes:

- Routinely evaluating the adequacy and effectiveness of security policies, procedures, and controls.
- Ensuring that effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual security incidents or through security alerts issued by FedCIRC, vendors, and other trusted sources.

Routine evaluations and response to identified vulnerabilities are important elements of risk management, which includes identifying, acknowledging, and responding, as appropriate, to changes in risk factors (e.g., computing environment, data sensitivity) and ensuring that security policies and procedures are appropriate and are operating as intended on an ongoing basis.

Routine self-assessments are an important means of identifying inappropriate or ineffective security procedures and controls, reminding employees of their security-related responsibilities, and demonstrating management's commitment to security. Self-assessments can be performed by agency staff or by contractors or others engaged by agency management. Independent audits such as those arranged by the General Accounting Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but should not be viewed as a substitute for evaluations initiated by agency management.

To be effective, routine evaluations must include tests and examinations of key controls. Reviews of documentation, walk-throughs of agency facilities, and interviews with agency personnel, while providing useful information, are not sufficient to ensure that controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users (e.g., external parties, hackers) gaining access. Similar to levels 1 through 3, to be meaningful, evaluations must include security controls of interconnected assets, e.g., network supporting applications being tested.

When assets are first implemented or are modified, they should be tested and certified to ensure that controls are initially operating as intended. (This would occur at Level 3.) Requirements for subsequent testing and recertification should be integrated into an agency's ongoing test and evaluation program.

In addition to test results, agency evaluations should consider information gleaned from records of potential and actual security incidents and from security alerts, such as those issued by software vendors. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risks.

The criteria listed below should be applied to each control area listed in the NIST questionnaire to determine if the asset is being effectively evaluated.

5.2 Criteria

Level 4 criteria are listed below.

Criteria for Level 4

a. **Effective program for evaluating adequacy and effectiveness of security policies, procedures, and controls.** Evaluation requirements, including requirements regarding the type and frequency of testing, should be documented, approved, and effectively implemented. The frequency and rigor with which individual controls are tested should depend on the risks that will be posed if the controls are not operating effectively. At a minimum, controls should be evaluated whenever significant system changes are made or when other risk factors, such as the sensitivity of data processed, change. Even controls for inherently low-risk operations should be tested at a minimum of every 3 years.

b. Mechanisms for identifying vulnerabilities revealed by security incidents or security alerts. Agencies should routinely analyze security incident records, including any records of anomalous or suspicious activity that may reveal security vulnerabilities. In addition, they should review security alerts issued by FedCIRC, vendors, and others.

c. Process for reporting significant security weaknesses and ensuring effective remedial action. *Such a process should provide for routine reports to senior management on weaknesses identified through testing or other means, development of action plans, allocation of needed resources, and follow-up reviews to ensure that remedial actions have been effective. Expedited processes should be implemented for especially significant weaknesses that may present undue risk if not addressed immediately.*

FULLY INTEGRATED PROCEDURES AND CONTROLS—LEVEL 5

Description

Level 5 of the Framework includes:

- A comprehensive security program that is an integral part of an agency's organizational culture.
- Decision-making based on cost, risk, and mission impact.

The consideration of IT security is pervasive in the culture of a level 5 asset. A proven life-cycle methodology is implemented and enforced and an ongoing program to identify and institutionalize best practices has been implemented. There is active support from senior management. Decisions and actions that are part of the IT life cycle include:

- Improving security program
- Improving security program procedures
- Improving or refining security controls
- Adding security controls
- Integrating security within existing and evolving IT architecture
- Improving mission processes and risk management activities

Each of these decisions result from a continuous improvement and refinement program instilled within the organization. At level 5, the understanding of mission-related risks and the associated costs of reducing these risks are considered with a full range of implementation options to achieve maximum mission cost-effectiveness of security measures. Entities should apply the principle of selecting controls that offer the lowest cost implementation while offering adequate risk mitigation, versus high cost implementation and low risk mitigation. The criteria listed below should be used to assess whether a specific control contained in the NIST questionnaire has been fully implemented.

Criteria

Level 5 criteria describe components of a fully integrated security program.

Criteria for Level 5

a. There is an active enterprise-wide security program that achieves cost-effective security.
b. IT security is an integrated practice within the asset.
c. Security vulnerabilities are understood and managed.
d. Threats are continually re-evaluated, and controls adapted to changing security environment.
e. Additional or more cost-effective security alternatives are identified as the need arises.
f. Costs and benefits of security are measured as precisely as practicable.
g. Status metrics for the security program are established and met.

FUTURE OF THE FRAMEWORK

This version of the Framework primarily addresses security management issues. It describes a process for agencies to assess their compliance with long-standing basic requirements and guidance. With the Framework in place, agencies will have an approach to begin the assessment process. The NIST questionnaire provides the tool to determine whether agencies are meeting these requirements and following the guidance.

The Framework is not static; it is a living document. Revisions will focus on expanding, refining, and providing more granularity for existing criteria. In addition, the establishment of a similar companion framework devoted to the evolution of agency electronic privacy polices may be considered in time.

The Framework can be viewed as both an auditing tool and a management tool. A balance between operational needs and cost effective security for acceptable risk will need to be made to achieve an adequate level of security.

Currently, the NIST self-assessment tool is under development and will be available in 2001. Appendix A provides a sample questionnaire to assist agencies until NIST officially releases the questionnaire.

APPENDIX A

Conceptual Sample of NIST Self-Assessment Questionnaire

Below is a conceptual sample of the Hypothetical Government Agency's (HGA) completion of the NIST questionnaire for their Training Database. Before the questionnaire was completed, the sensitivity of the information stored within, processed by and transmitted by this asset was assessed. The premise behind determining the level of sensitivity is that each asset owner is responsible for determining what level of risk is acceptable, and which specific security controls are necessary to provide adequate security.

The sensitivity of this asset was determined to be high for confidentiality and low for integrity and availability. The confidentiality of the system is high due to the system containing personnel information. Employee social security numbers, course lists, and grades are contained in the system. The integrity of the database is considered low because if the information were modified by unauthorized, unanticipated or unintentional means, employees, who can read their own training file, would detect the modifications. The availability of the system is considered low because hard copies of the training forms are available as a backup.

The questionnaire was completed for the database with the understanding that security controls that protect the integrity or availability of the data did not have to be rigidly applied. The questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control. There may be certain situations where management will grant a waiver either because compensating controls exist or because the benefits of operating without the control (at least temporarily) outweigh the risk of waiting for full control implementation. Alternatively, there may be times where management implements more stringent controls than generally applied elsewhere. In the example provided the specific control objectives for personnel security and for authentication were assessed. The questionnaire is an excerpt and by no means contains all the questions that would be asked in the area of personnel security and authentication. For brevity, only a few questions were provided in this sample.

An analysis of the levels checked determined that the agency should target improving their background screening implementation and testing. System administrators, programmers, and managers should all have background checks completed prior to accessing the system. The decision to allow access prior to screening was made and checked in the *Risk Based Decision Made* box. Because this box was checked, there should be specific controls implemented to ensure access is not abused, i.e., access is reviewed daily through audit trails, and users have minimal system authority.

Additionally, HGA should improve implementing and testing their password procedures because of the strong need for confidentiality. Without good password management, passwords can be easily guessed and access to the system obtained. The questionnaire's list of objectives is incomplete for both personnel security controls and for authentication controls. Even though the sample is lacking many controls, the completed questionnaire clearly depicts that HGA has policies and procedures in place but there is a strong need for implementing, testing, and reviewing the procedures and controls. The sample indicates that the Training Database would be at level 2.

Category of Sensitivity	Confidentiality	Integrity	Availability
High	X		
Medium			
Low		X	X

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made
Personnel Security						
Are all positions reviewed for sensitivity level?	X	X	X			
appropriate background screening for assigned positions completed prior to granting access?	X	X				X
Are there conditions for allowing system access prior to completion of screening?	X	X				

(Continued)

Category of Sensitivity	Confidentiality	Integrity	Availability
High	X		
Medium			
Low		X	X

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision MadeIs
Are sensitive functions divided among different individuals?	X	X	X			
Are mechanisms in place for holding usersresponsible for their actions?	X	X				
Are termination procedures established?	X	X				
Authentication						
Are passwords, tokens, or biometrics used?	X	X	X			
Do passwords contain alpha numeric, upper/ lower case, and special characters?	X	X				
Are passwords changed at least every ninety days or earlier if needed?	X	X				
Is there guidance for handling lost and compromised passwords?	X	X				
Are passwords transmitted and stored with one-way encryption?	X	X				
Is there a limit to the number of invalid access attempts that may occur for a given user?	X	X				

REFERENCES

Automated Information Systems Security Program Handbook (Release 2.0, May 1994), Department of Health and Human Services, May 1994.

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

Paperwork Reduction Act of 1995, 35 U.S. Code 44, January 4, 1995.

Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Swanson, Marianne and Barbara Guttman, NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP), Gaithersburg, MD, National Institute of Standards and Technology, September 20, 1995.

Swanson, Marianne and Federal Computer Security Program Managers' Forum Working Group, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.

TERMINOLOGY

Acceptable Risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls.

Accreditation is synonymous with the term **authorize processing**. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment.

It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also***Authorize Processing, Certification,*** and ***Designated Approving Authority***.

Asset is a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.

Authorize Processing occurs when management authorizes in writing a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system the management official accepts the risks associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority***.

Availability Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Awareness, Training, and Education includes (1) awareness programs set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in IT security.

Certification is synonymous with the term **authorize processing**. Certification is a major consideration prior to authorizing processing, but not the only consideration. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See also***Accreditation*** and***Authorize Processing***.

General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information Owner is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Material Weakness or ***significant weakness*** is used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Operational Controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Policy a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Procedures are contained in a document that focuses on the security control areas and management's position.

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal government equipment, assignment and limitation of system privileges, and individual accountability.

Sensitive Information refers to information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled.

Sensitivity an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability that is determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

System is a generic term used for briefness to mean either a major application or a general support system.

System Operational Status is either (1) Operational—system is currently in operation, (2) Under Development—system is currently under design, development, or implementation, or (3) Undergoing a Major Modification—system is currently undergoing a major conversion or transition.

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat is an event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

Vulnerability is a flaw or weakness that may allow harm to occur to an IT system or activity.

APPENDIX D—REFERENCES

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, "Government Information Security Reform," October 28, 2000.

Department of State, Draft Best Security Practices Checklist Appendix A, January 22, 2001.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

ISSO 17799, A Code of Practice for Information Security Management (British Standard 7799),

National Communications System, Public Switched Network Security Assessment Guidelines, September 2000.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

Paperwork Reduction Act of 1995, 35 U.S. Code 44, January 4, 1995.

Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Stoneburner, Gary, Draft –Rev. A NIST Special Publication 800-30, Risk Management Guide, February 16, 2001.

Swanson, Marianne and Barbara Guttman, NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP), Gaithersburg, MD, National Institute of Standards and Technology, September 20, 1995.

Swanson, Marianne and Federal Computer Security Program Managers' Forum Working Group, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.

NOTES

1. OMB Circular A-130, Appendix III defines general support system or "system" in similar terms.

2. Draft NIST Special Publication 800-30, "Risk Management Guidance" dated June 2001.

3. FedCIRC (Federal Computer Incident Response Capability) is the U.S. Government's focal point for handling computer security-related incidents.

4. NIPC's mission is to serve as the U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures.

5. The NIST Self-assessment Questionnaire will be issued in 2001 as a NIST Special Publication.

EMERGENCY MANAGEMENT GUIDE FOR BUSINESS AND INDUSTRY

A Step-by-Step Approach to Emergency Planning, Response and Recovery for Companies of All Sizes

FEMA 141/October 1993

A hurricane blasts through South Florida causing more than $25 billion in damages.

A fire at a food processing plant results in 25 deaths, a company out of business, and a small town devastated.

A bombing in the World Trade Center results in six deaths, hundreds of injuries, and the evacuation of 40,000 people.

A blizzard shuts down much of the East Coast for days. More than 150 lives are lost and millions of dollars in damages incurred.

Every year emergencies take their toll on business and industry—in lives and dollars. But something can be done. Business and industry can limit injuries and damages and return more quickly to normal operations if they plan ahead.

ABOUT THIS GUIDE

This guide provides step-by-step advice on how to create and maintain a comprehensive emergency management program. It can be used by manufacturers, corporate offices, retailers, utilities or any organization where a sizable number of people work or gather.

Whether you operate from a high-rise building or an industrial complex; whether you own, rent or lease your property; whether you are a large or small company; the concepts in this guide will apply.

To begin, you need not have in-depth knowledge of emergency management. What you need is the authority to create a plan and a commitment from the chief executive officer to make emergency management part of your corporate culture.

If you already have a plan, use this guide as a resource to assess and update your plan.

The guide is organized as follows:

Section 1: 4 Steps in the Planning Process—how to form a planning team; how to conduct a vulnerability analysis; how to develop a plan; and how to implement the plan. The information can be applied to virtually any type of business or industry.

Section 2: Emergency Management Considerations—how to build such emergency management capabilities as life safety, property protection, communications and community outreach.

Section 3: Hazard-Specific Information—technical information about specific hazards your facility may face.

Section 4: Information Sources—where to turn for additional information.

WHAT IS AN EMERGENCY?

An emergency is any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public image.

Obviously, numerous events can be "emergencies," including:

- Fire
- Hazardous materials incident
- Flood or flash flood
- Hurricane
- Tornado
- Winter storm
- Earthquake
- Communications failure
- Radiological accident
- Civil disturbance
- Loss of key supplier or customer
- Explosion

The term "disaster" has been left out of this document because it lends itself to a preconceived notion of a large-scale event, usually a "natural disaster." In fact, each event must be addressed within the context of the impact it has on the company and the community. What might constitute a nuisance to a large industrial facility could be a "disaster" to a small business.

WHAT IS EMERGENCY MANAGEMENT?

Emergency management is the process of preparing for, mitigating, responding to and recovering from an emergency.

Emergency management is a dynamic process. Planning, though critical, is not the only component. Training, conducting drills, testing equipment and coordinating activities with the community are other important functions.

MAKING THE "CASE" FOR EMERGENCY MANAGEMENT

To be successful, emergency management requires upper management support. The chief executive sets the tone by authorizing planning to take place and directing senior management to get involved.

When presenting the "case" for emergency management, avoid dwelling on the negative effects of an emergency (e.g., deaths, fines, criminal prosecution) and emphasize the positive aspects of preparedness. For example:

- It helps companies fulfill their moral responsibility to protect employees, the community and the environment.
- It facilitates compliance with regulatory requirements of Federal, State and local agencies.
- It enhances a company's ability to recover from financial losses, regulatory fines, loss of market share, damages to equipment or products or business interruption.
- It reduces exposure to civil or criminal liability in the event of an incident.
- It enhances a company's image and credibility with employees, customers, suppliers and the community.
- It may reduce your insurance premiums.

SECTION 1: 4 STEPS IN THE PLANNING PROCESS

Establish A Planning Team

There must be an individual or group in charge of developing the emergency management plan. The following is guidance for making the appointment.

Form the Team

The size of the planning team will depend on the facility's operations, requirements and resources. Usually involving a group of people is best because:

- It encourages participation and gets more people invested in the process.
- It increases the amount of time and energy participants are able to give.
- It enhances the visibility and stature of the planning process.
- It provides for a broad perspective on the issues.

Determine who can be an active member and who can serve in an advisory capacity. In most cases, one or two people will be doing the bulk of the work. At the very least, you should obtain input from all functional areas.

Remember:

- Upper management
- Line management
- Labor
- Human Resources
- Engineering and maintenance
- Safety, health and environmental affairs
- Public information officer
- Security
- Community relations
- Sales and marketing
- Legal
- Finance and purchasing

Have participants appointed in writing by upper management.

Their job descriptions could also reflect this assignment.

Establish Authority

Demonstrate management's commitment and promote an atmosphere of cooperation by "authorizing" the planning group to take the steps necessary to develop a plan. The group should be led by the chief executive or the plant manager.

Establish a clear line of authority between group members and the group leader, though not so rigid as to prevent the free flow of ideas.

Issue a Mission Statement

Have the chief executive or plant manager issue a mission statement to demonstrate the company's commitment to emergency management. The statement should:

- Define the purpose of the plan and indicate that it will involve the entire organization
- Define the authority and structure of the planning group

Establish a Schedule and Budget

Establish a work schedule and planning deadlines. Timelines can be modified as priorities become more clearly defined.

Develop an initial budget for such things as research, printing, seminars, consulting services and other expenses that may be necessary during the development process.

Analyze Capabilities and Hazards

This step entails gathering information about current capabilities and about possible hazards and emergencies, and then conducting a vulnerability analysis to determine the facility's capabilities for handling emergencies.

Where Do You Stand Right Now?

Review Internal Plans and Policies

Documents to look for include:

- Evacuation plan
- Fire protection plan
- Safety and health program
- Environmental policies
- Security procedures
- Insurance programs
- Finance and purchasing procedures
- Plant closing policy
- Employee manuals
- Hazardous materials plan
- Process safety assessment
- Risk management plan
- Capital improvement program
- Mutual aid agreements

Meet with Outside Groups

Meet with government agencies, community organizations and utilities. Ask about potential emergencies and about plans and available resources for responding to them. Sources of information include:

- Community emergency management office
- Mayor or Community Administrator's office
- Local Emergency Planning Committee (LEPC)
- Fire Department
- Police Department
- Emergency Medical Services organizations
- American Red Cross
- National Weather Service
- Public Works Department
- Planning Commission
- Telephone companies
- Electric utilities
- Neighboring businesses

Identify Codes and Regulations

Identify applicable Federal, State and local regulations such as:

- Occupational safety and health regulations
- Environmental regulations
- Fire codes
- Seismic safety codes
- Transportation regulations
- Zoning regulations
- Corporate policies

Identify Critical Products, Services and Operations

You'll need this information to assess the impact of potential emergencies and to determine the need for backup systems. Areas to review include:

- Company products and services and the facilities and equipment needed to produce them
- Products and services provided by suppliers, especially sole source vendors
- Lifeline services such as electrical power, water, sewer, gas, telecommunications and transportation
- Operations, equipment and personnel vital to the continued functioning of the facility

Identify Internal Resources and Capabilities

Resources and capabilities that could be needed in an emergency include:

- Personnel—fire brigade, hazardous materials response team, emergency medical services, security, emergency management group, evacuation team, public information officer
- Equipment—fire protection and suppression equipment, communications equipment, first aid supplies, emergency supplies, warning systems, emergency power equipment, decontamination equipment
- Facilities—emergency operating center, media briefing area, shelter areas, first-aid stations, sanitation facilities
- Organizational capabilities—training, evacuation plan, employee support system
- Backup systems—arrangements with other facilities to provide for:
  - Payroll
  - Communications
  - Production
  - Customer services
  - Shipping and receiving
  - Information systems support

- Emergency power
- Recovery support

Identify External Resources

There are many external resources that could be needed in an emergency. In some cases, formal agreements may be necessary to define the facility's relationship with the following:

- Local emergency management office
- Fire Department
- Hazardous materials response organization
- Emergency medical services
- Hospitals
- Local and State police
- Community service organizations
- Utilities
- Contractors
- Suppliers of emergency equipment
- Insurance carriers

Do an Insurance Review

Meet with insurance carriers to review all policies. (See Section 2: Recovery and Restoration.)

Conduct a Vulnerability Analysis

The next step is to assess the vulnerability of your facility—the probability and potential impact of each emergency. Use the Vulnerability Analysis Chart in the appendix section to guide the process, which entails assigning probabilities, estimating impact and assessing resources, using a numerical system. The lower the score the better.

List Potential Emergencies

In the first column of the chart, list all emergencies that could affect your facility, including those identified by your local emergency management office. Consider both:

- Emergencies that could occur within your facility
- Emergencies that could occur in your community

Below are some other factors to consider.

- Historical—What types of emergencies have occurred in the community, at this facility and at other facilities in the area?

  - Fires
  - Severe weather
  - Hazardous material spills
  - Transportation accidents
  - Earthquakes
  - Hurricanes
  - Tornadoes
  - Terrorism
  - Utility outages

- Geographic—What can happen as a result of the facility's location? Keep in mind:
  - Proximity to flood plains, seismic faults and dams
  - Proximity to companies that produce, store, use or transport hazardous materials
  - Proximity to major transportation routes and airports
  - Proximity to nuclear power plants

- Technological—What could result from a process or system failure? Possibilities include:
  - Fire, explosion, hazardous materials incident
  - Safety system failure
  - Telecommunications failure
  - Computer system failure
  - Power failure
  - Heating/cooling system failure
  - Emergency notification system failure

- Human Error—What emergencies can be caused by employee error? Are employees trained to work safely? Do they know what to do in an emergency?

  Human error is the single largest cause of workplace emergencies and can result from:
  - Poor training
  - Poor maintenance
  - Carelessness
  - Misconduct
  - Substance abuse
  - Fatigue

- Physical—What types of emergencies could result from the design or construction of the facility? Does the physical facility enhance safety? Consider:
  - The physical construction of the facility
  - Hazardous processes or byproducts
  - Facilities for storing combustibles
  - Layout of equipment

  - Lighting
  - Evacuation routes and exits
  - Proximity of shelter areas

- Regulatory—What emergencies or hazards are you regulated to deal with?

Analyze each potential emergency from beginning to end. Consider what could happen as a result of:

  - Prohibited access to the facility
  - Loss of electric power
  - Communication lines down
  - Ruptured gas mains
  - Water damage
  - Smoke damage
  - Structural damage
  - Air or water contamination
  - Explosion
  - Building collapse
  - Trapped persons
  - Chemical release

Estimate Probability

In the Probability column, rate the likelihood of each emergency's occurrence. This is a subjective consideration, but useful nonetheless.

Use a simple scale of 1 to 5 with 1 as the lowest probability and 5 as the highest.

Assess the Potential Human Impact

Analyze the potential human impact of each emergency—the possibility of death or injury.

Assign a rating in the Human Impact column of the Vulnerability Analysis Chart. Use a 1 to 5 scale with 1 as the lowest impact and 5 as the highest.

Assess the Potential Property Impact

Consider the potential property for losses and damages. Again, assign a rating in the Property Impact column, 1 being the lowest impact and 5 being the highest. Consider:

- Cost to replace
- Cost to set up temporary replacement
- Cost to repair

Assess the Potential Business Impact

Consider the potential loss of market share. Assign a rating in the Business Impact column. Again, 1 is the lowest impact and 5 is the highest. Assess the impact of:

- Business interruption
- Employees unable to report to work
- Customers unable to reach facility
- Company in violation of contractual agreements
- Imposition of fines and penalties or legal costs
- Interruption of critical supplies
- Interruption of product distribution

Assess Internal and External Resources

Next assess your resources and ability to respond. Assign a score to your Internal Resources and External Resources. The lower the score the better.

To help you do this, consider each potential emergency from beginning to end and each resource that would be needed to respond. For each emergency ask these questions:

- Do we have the needed resources and capabilities to respond?
- Will external resources be able to respond to us for this emergency as quickly as we may need them, or will they have other priority areas to serve?

If the answers are yes, move on to the next assessment. If the answers are no, identify what can be done to correct the problem. For example, you may need to:

- Develop additional emergency procedures
- Conduct additional training
- Acquire additional equipment
- Establish mutual aid agreements
- Establish agreements with specialized contractors

Add the Columns

Total the scores for each emergency. The lower the score the better. While this is a subjective rating, the comparisons will help determine planning and resource priorities—the subject of the pages to follow.

Develop The Plan

You are now ready to develop an emergency management plan. This section describes how.

Plan Components

Your plan should include the following basic components.

Executive Summary

The executive summary gives management a brief overview of:

- The purpose of the plan
- The facility's emergency management policy
- Authorities and responsibilities of key personnel
- The types of emergencies that could occur
- Where response operations will be managed

Emergency Management Elements

This section of the plan briefly describes the facility's approach to the core elements of emergency management, which are:

- Direction and control
- Communications
- Life safety
- Property protection
- Community outreach
- Recovery and restoration
- Administration and logistics

These elements, which are described in detail in Section 2, are the foundation for the emergency procedures that your facility will follow to protect personnel and equipment and resume operations.

Emergency Response Procedures

The procedures spell out how the facility will respond to emergencies. Whenever possible, develop them as a series of checklists that can be quickly accessed by senior management, department heads, response personnel and employees.

Determine what actions would be necessary to:

- Assess the situation
- Protect employees, customers, visitors, equipment, vital records and other assets, particularly during the first three days
- Get the business back up and running

Specific procedures might be needed for any number of situations such as bomb threats or tornadoes, and for such functions as:

- Warning employees and customers
- Communicating with personnel and community responders
- Conducting an evacuation and accounting for all persons in the facility
- Managing response activities
- Activating and operating an emergency operations center
- Fighting fires
- Shutting down operations
- Protecting vital records
- Restoring operations

Support Documents

Documents that could be needed in an emergency include:

- Emergency call lists—lists (wallet size if possible) of all persons on and off site who would be involved in responding to an emergency, their responsibilities and their 24-hour telephone numbers
- Building and site maps that indicate:
  - Utility shutoffs
  - Water hydrants
  - Water main valves
  - Water lines
  - Gas main valves
  - Gas lines
  - Electrical cutoffs
  - Electrical substations
  - Storm drains
  - Sewer lines
  - Location of each building (include name of building, street name and number)
  - Floor plans
  - Alarm and enunciators
  - Fire extinguishers
  - Fire suppression systems
  - Exits
  - Stairways
  - Designated escape routes
  - Restricted areas
  - Hazardous materials (including cleaning supplies and chemicals)
  - High-value items
- Resource lists—lists of major resources (equipment, supplies, services) that could be needed in an emergency; mutual aid agreements with other companies and government agencies

The Development Process

The following is guidance for developing the plan.

Identify Challenges and Prioritize Activities

Determine specific goals and milestones. Make a list of tasks to be performed, by whom and when. Determine how you will address the problem areas and resource shortfalls that were identified in the vulnerability analysis.

Write the Plan

Assign each member of the planning group a section to write. Determine the most appropriate format for each section.

Establish an aggressive timeline with specific goals. Provide enough time for completion of work, but not so much as to allow assignments to linger. Establish a schedule for:

- First draft
- Review
- Second draft
- Tabletop exercise
- Final draft
- Printing
- Distribution

Establish a Training Schedule

Have one person or department responsible for developing a training schedule for your facility. For specific ideas about training, refer to Step 4.

Coordinate with Outside Organizations

Meet periodically with local government agencies and community organizations. Inform appropriate government agencies that you are creating an emergency management plan. While their official approval may not be required, they will likely have valuable insights and information to offer.

Determine State and local requirements for reporting emergencies, and incorporate them into your procedures.

Determine protocols for turning control of a response over to outside agencies. Some details that may need to be worked out are:

- Which gate or entrance will responding units use?
- Where and to whom will they report?
- How will they be identified?
- How will facility personnel communicate with outside responders?
- Who will be in charge of response activities?

Determine what kind of identification authorities will require to allow your key personnel into your facility during an emergency.

Maintain Contact with Other Corporate Offices

Communicate with other offices and divisions in your company to learn:

- Their emergency notification requirements
- The conditions where mutual assistance would be necessary
- How offices will support each other in an emergency
- Names, telephone numbers and pager numbers of key personnel

Incorporate this information into your procedures.

Review, Conduct Training and Revise

Distribute the first draft to group members for review. Revise as needed.

For a second review, conduct a tabletop exercise with management and personnel who have a key emergency management responsibility. In a conference room setting, describe an emergency scenario and have participants discuss their responsibilities and how they would react to the situation. Based on this discussion, identify areas of confusion and overlap, and modify the plan accordingly.

Seek Final Approval

Arrange a briefing for the chief executive officer and senior management and obtain written approval.

Distribute the Plan

Place the final plan in three-ring binders and number all copies and pages. Each individual who receives a copy should be required to sign for it and be responsible for posting subsequent changes.

Determine which sections of the plan would be appropriate to show to government agencies (some sections may refer to corporate secrets or include private listings of names, telephone numbers or radio frequencies).

Distribute the final plan to:

- Chief executive and senior managers
- Key members of the company's emergency response organization
- Company headquarters
- Community emergency response agencies (appropriate sections)

Have key personnel keep a copy of the plan in their homes.

Inform employees about the plan and training schedule.

Implement the Plan

Implementation means more than simply exercising the plan during an emergency. It means acting on recommendations made during the vulnerability analysis, integrating the plan into company operations, training employees and evaluating the plan.

Integrate the Plan Into Company Operations

Emergency planning must become part of the corporate culture.

Look for opportunities to build awareness; to educate and train personnel; to test procedures; to involve all levels of management, all departments and the community in the planning process; and to make emergency management part of what personnel do on a day-to-day basis.

Test how completely the plan has been integrated by asking:

- How well does senior management support the responsibilities outlined in the plan?
- Have emergency planning concepts been fully incorporated into the facility's accounting, personnel and financial procedures?
- How can the facility's processes for evaluating employees and defining job classifications better address emergency management responsibilities?
- Are there opportunities for distributing emergency preparedness information through corporate newsletters, employee manuals or employee mailings?
- What kinds of safety posters or other visible reminders would be helpful?
- Do personnel know what they should do in an emergency?
- How can all levels of the organization be involved in evaluating and updating the plan?

Conduct Training

Everyone who works at or visits the facility requires some form of training. This could include periodic employee discussion sessions to review procedures, technical training in equipment use for emergency responders, evacuation drills and full-scale exercises. Below are basic considerations for developing a training plan.

Planning Considerations

Assign responsibility for developing a training plan. Consider the training and information needs for employees, contractors, visitors, managers and those with an emergency response role identified in the plan.

Determine for a 12 month period:

- Who will be trained
- Who will do the training
- What training activities will be used
- When and where each session will take place
- How the session will be evaluated and documented

Use the Training Drills and Exercises Chart in the appendix section to schedule training activities or create one of your own.

Consider how to involve community responders in training activities.

Conduct reviews after each training activity. Involve both personnel and community responders in the evaluation process.

Training Activities

Training can take many forms:

- Orientation and Education Sessions—These are regularly scheduled discussion sessions to provide information, answer questions and identify needs and concerns.

- Tabletop Exercise—Members of the emergency management group meet in a conference room setting to discuss their responsibilities and how they would react to emergency scenarios. This is a cost-effective and efficient way to identify areas of overlap and confusion before conducting more demanding training activities.
- Walk-through Drill—The emergency management group and response teams actually perform their emergency response functions. This activity generally involves more people and is more thorough than a tabletop exercise.
- Functional Drills—These drills test specific functions such as medical response, emergency notifications, warning and communications procedures and equipment, though not necessarily at the same time. Personnel are asked to evaluate the systems and identify problem areas.
- Evacuation Drill—Personnel walk the evacuation route to a designated area where procedures for accounting for all personnel are tested. Participants are asked to make notes as they go along of what might become a hazard during an emergency, e.g., stairways cluttered with debris, smoke in the hallways. Plans are modified accordingly.
- Full-scale Exercise—A real-life emergency situation is simulated as closely as possible. This exercise involves company emergency response personnel, employsees, management and community response organizations.

Employee Training

General training for all employees should address:

- Individual roles and responsibilities
- Information about threats, hazards and protective actions
- Notification, warning and communications procedures
- Means for locating family members in an emergency
- Emergency response procedures
- Evacuation, shelter and accountability procedures
- Location and use of common emergency equipment
- Emergency shutdown procedures

The scenarios developed during the vulnerability analysis can serve as the basis for training events.

Evaluate and Modify the Plan

Conduct a formal audit of the entire plan at least once a year. Among the issues to consider are:

- How can you involve all levels of management in evaluating and updating the plan?
- Are the problem areas and resource shortfalls identified in the vulnerability analysis being sufficiently addressed?

- Does the plan reflect lessons learned from drills and actual events?
- Do members of the emergency management group and emergency response team understand their respective responsibilities? Have new members been trained?
- Does the plan reflect changes in the physical layout of the facility? Does it reflect new facility processes?
- Are photographs and other records of facility assets up to date?
- Is the facility attaining its training objectives?
- Have the hazards in the facility changed?
- Are the names, titles and telephone numbers in the plan current?
- Are steps being taken to incorporate emergency management into other facility processes?
- Have community agencies and organizations been briefed on the plan? Are they involved in evaluating the plan?

In addition to a yearly audit, evaluate and modify the plan at these times:

- After each training drill or exercise
- After each emergency
- When personnel or their responsibilities change
- When the layout or design of the facility changes
- When policies or procedures change

Remember to brief personnel on changes to the plan.

SECTION 2: EMERGENCY MANAGEMENT CONSIDERATIONS

Direction and Control

Someone must be in charge in an emergency. The system for managing resources, analyzing information and making decisions in an emergency is called direction and control.

The direction and control system described below assumes a facility of sufficient size. Your facility may require a less sophisticated system, though the principles described here will still apply.

The configuration of your system will depend on many factors. Larger industries may have their own fire team, emergency medical technicians or hazardous materials team, while smaller organizations may need to rely on mutual aid agreements. They may also be able to consolidate positions or combine responsibilities. Tenants of office buildings or industrial parks may be part of an emergency management program for the entire facility.

Emergency Management Group (EMG)

The EMG is the team responsible for the big picture. It controls all incident-related activities. The Incident Commander (IC) oversees the technical aspects of the response.

The EMG supports the IC by allocating resources and by interfacing with the community, the media, outside response organizations and regulatory agencies.

The EMG is headed by the Emergency Director (ED), who should be the facility manager. The ED is in command and control of all aspects of the emergency. Other EMG members should be senior managers who have the authority to:

- Determine the short-and long-term effects of an emergency
- Order the evacuation or shutdown of the facility
- Interface with outside organizations and the media
- Issue press releases

The relationship between the EMG and the IC is shown in Figure 1.

Incident Command System (ICS)

The ICS was developed specifically for the fire service, but its principles can be applied to all emergencies. The ICS provides for coordinated response and a clear chain of command and safe operations.

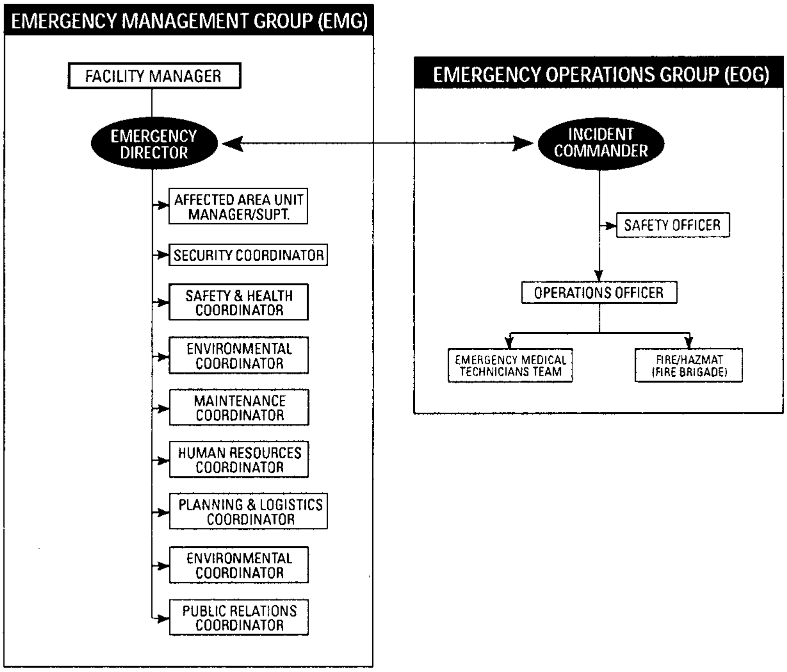

EMERGENCY MANAGEMENT GROUP (EMG)
FACILITY MANAGER
EMERGENCY DIRECTOR
AFFECTED AREA UNIT MANAGER/SUPT.
SECURITY COORDINATOR
SAFETY & HEALTH COORDINATOR
ENVIRONMENTAL COORDINATOR
MAINTENANCE COORDINATOR
HUMAN RESOURCES COORDINATOR
PLANNING & LOGISTICS COORDINATOR
ENVIRONMENTAL COORDINATOR
PUBLIC RELATIONS COORDINATOR
EMERGENCY OPERATIONS GROUP (EOG)
INCIDENT COMMANDER
SAFETY OFFICER
OPERATIONS OFFICER
EMERGENCY MEDICAL TECHNICIANS TEAM
FIRE/HAZMAT (FIRE BRIGADE)

Figure 1 Relationship between the EMG and the IC.

The Incident Commander (IC) is responsible for front-line management of the incident, for tactical planning and execution, for determining whether outside assistance is needed and for relaying requests for internal resources or outside assistance through the Emergency Operations Center (EOC).

The IC can be any employee, but a member of management with the authority to make decisions is usually the best choice.

The IC must have the capability and authority to:

- Assume command
- Assess the situation
- Implement the emergency management plan
- Determine response strategies
- Activate resources
- Order an evacuation
- Oversee all incident response activities
- Declare that the incident is "over"

Emergency Operations Center (EOC)

The EOC serves as a centralized management center for emergency operations. Here, decisions are made by the EMG based upon information provided by the IC and other personnel. Regardless of size or process, every facility should designate an area where decision makers can gather during an emergency.

The EOC should be located in an area of the facility not likely to be involved in an incident, perhaps the security department, the manager's office, a conference room or the training center. An alternate EOC should be designated in the event that the primary location is not usable.

Each facility must determine its requirements for an EOC based upon the functions to be performed and the number of people involved. Ideally, the EOC is a dedicated area equipped with communications equipment, reference materials, activity logs and all the tools necessary to respond quickly and appropriately to an emergency.

Planning Considerations

To develop a direction and control system:

- Define the duties of personnel with an assigned role. Establish procedures for each position. Prepare checklists for all procedures.
- Define procedures and responsibilities for fire fighting, medical and health, and engineering.
- Determine lines of succession to ensure continuous leadership, authority and responsibility in key positions.
- Determine equipment and supply needs for each response function.
- At a minimum, assign all personnel responsibility for:
  - Recognizing and reporting an emergency
  - Warning other employees in the area

  - Taking security and safety measures
  - Evacuating safely
- Provide training.

Security

Isolation of the incident scene must begin when the emergency is discovered. If possible, the discoverer should attempt to secure the scene and control access, but no one should be placed in physical danger to perform these functions.

Basic security measures include:

- Closing doors or windows
- Establishing temporary barriers with furniture after people have safely evacuated
- Dropping containment materials (sorbent pads, etc.) in the path of leaking materials
- Closing file cabinets or desk drawers

Only trained personnel should be allowed to perform advanced security measures. Access to the facility, the EOC and the incident scene should be limited to persons directly involved in the response.

Coordination of Outside Response

In some cases, laws, codes, prior agreements or the very nature of the emergency require the IC to turn operations over to an outside response organization.

When this happens, the protocols established between the facility and outside response organizations are implemented. The facility's IC provides the community's IC a complete report on the situation.

The facility IC keeps track of which organizations are on-site and how the response is being coordinated. This helps increase personnel safety and accountability, and prevents duplication of effort.

Communications

Communications are essential to any business operation. A communications failure can be a disaster in itself, cutting off vital business activities.

Communications are needed to report emergencies, to warn personnel of the danger, to keep families and off-duty employees informed about what's happening at the facility to coordinate response actions and to keep in contact with customers and suppliers.

Contingency Planning

Plan for all possible contingencies from a temporary or short-term disruption to a total communications failure.

- Consider the everyday functions performed by your facility and the communications, both voice and data, used to support them.
- Consider the business impact if your communications were inoperable. How would this impact your emergency operations?
- Prioritize all facility communications. Determine which should be restored first in an emergency.
- Establish procedures for restoring communications systems.
- Talk to your communications vendors about their emergency response capabilities. Establish procedures for restoring services.
- Determine needs for backup communications for each business function. Options include messengers, telephones, portable microwave, amateur radios, point-to-point private lines, satellite, high-frequency radio.

Emergency Communications

Consider the functions your facility might need to perform in an emergency and the communications systems needed to support them.

Consider communications between:

- Emergency responders
- Responders and the Incident Commander (IC)
- The IC and the Emergency Operations Center (EOC)
- The IC and employees
- The EOC and outside response organizations
- The EOC and neighboring businesses
- The EOC and employees' families
- The EOC and customers
- The EOC and media

Methods of communication include:

- Messenger
- Telephone
- Two-way radio
- FAX machine
- Microwave
- Satellite
- Dial-up modems
- Local area networks
- Hand signals

Family Communications

In an emergency, personnel will need to know whether their families are okay. Taking care of one's loved ones is always a first priority.

Make plans for communicating with employees' families in an emergency. Also, encourage employees to:

- Consider how they would communicate with their families in case they are separated from one another or injured in an emergency.
- Arrange for an out-of-town contact for all family members to call in an emergency.
- Designate a place to meet family members in case they cannot get home in an emergency.

Notification

Establish procedures for employees to report an emergency. Inform employees of procedures. Train personnel assigned specific notification tasks.

Post emergency telephone numbers near each telephone, on employee bulletin boards and in other prominent locations.

Maintain an updated list of addresses and telephone and pager numbers of key emergency response personnel (from within and outside the facility).

Listen for tornado, hurricane and other severe weather warnings issued by the National Weather Service.

Determine government agencies' notification requirements in advance. Notification must be made immediately to local government agencies when an emergency has the potential to affect public health and safety.

Prepare announcements that could be made over public address systems.

Warning

Establish a system for warning personnel of an emergency. The system should:

- Be audible or within view by all people in the facility
- Have an auxiliary power supply
- Have a distinct and recognizable signal

Make plans for warning persons with disabilities. For instance, a flashing strobe light can be used to warn hearing-impaired people.

Familiarize personnel with procedures for responding when the warning system is activated.

Establish procedures for warning customers, contractors, visitors and others who may not be familiar with the facility's warning system.

Test your facility's warning system at least monthly.

Life Safety

Protecting the health and safety of everyone in the facility is the first priority during an emergency.

Evacuation Planning

One common means of protection is evacuation. In the case of fire, an immediate evacuation to a predetermined area away from the facility may be necessary. In a hurricane, evacuation could involve the entire community and take place over a period of days.

To develop an evacuation policy and procedure:

- Determine the conditions under which an evacuation would be necessary.
- Establish a clear chain of command. Identify personnel with the authority to order an evacuation. Designate "evacuation wardens" to assist others in an evacuation and to account for personnel.
- Establish specific evacuation procedures. Establish a system for accounting for personnel. Consider employees' transportation needs for community-wide evacuations.
- Establish procedures for assisting persons with disabilities and those who do not speak English.
- Post evacuation procedures.
- Designate personnel to continue or shut down critical operations while an evacuation is underway. They must be capable of recognizing when to abandon the operation and evacuate themselves.
- Coordinate plans with the local emergency management office.

Evacuation Routes and Exits

Designate primary and secondary evacuation routes and exits. Have them clearly marked and well lit. Post signs.

Install emergency lighting in case a power outage occurs during an evacuation.

Ensure that evacuation routes and emergency exits are:

- Wide enough to accommodate the number of evacuating personnel
- Clear and unobstructed at all times
- Unlikely to expose evacuating personnel to additional hazards

Have evacuation routes evaluated by someone not in your organization.

Assembly Areas and Accountability

Obtaining an accurate account of personnel after a site evacuation requires planning and practice.

- Designate assembly areas where personnel should gather after evacuating.
- Take a head count after the evacuation. The names and last known locations of personnel not accounted for should be determined and given to the EOC. (Confusion in the assembly areas can lead to unnecessary and dangerous search and rescue operations.)

- Establish a method for accounting for non-employees such as suppliers and customers.
- Establish procedures for further evacuation in case the incident expands. This may consist of sending employees home by normal means or providing them with transportation to an off-site location.

Shelter

In some emergencies, the best means of protection is to take shelter either within the facility or away from the facility in a public building.

- Consider the conditions for taking shelter, e.g., tornado warning.
- Identify shelter space in the facility and in the community. Establish procedures for sending personnel to shelter.
- Determine needs for emergency supplies such as water, food and medical supplies.
- Designate shelter managers, if appropriate.
- Coordinate plans with local authorities.

Training and Information

Train employees in evacuation, shelter and other safety procedures. Conduct sessions at least annually or when:

- Employees are hired
- Evacuation wardens, shelter managers and others with special assignments are designated
- New equipment, materials or processes are introduced
- Procedures are updated or revised
- Exercises show that employee performance must be improved

Provide emergency information such as checklists and evacuation maps.
Post evacuation maps in strategic locations.
Consider the information needs of customers and others who visit the facility.

Family Preparedness

Consider ways to help employees prepare their families for emergencies. This will increase their personal safety and help the facility get back up and running. Those who are prepared at home will be better able to carry out their responsibilities at work.

Property Protection

Protecting facilities, equipment and vital records is essential to restoring operations once an emergency has occurred.

Planning Considerations

Establish procedures for:

- Fighting fires
- Containing material spills
- Closing or barricading doors and windows
- Shutting down equipment
- Covering or securing equipment
- Moving equipment to a safe location

Identify sources of backup equipment, parts and supplies.

Designate personnel to authorize, supervise and perform a facility shutdown. Train them to recognize when to abandon the effort.

Obtain materials to carry out protection procedures and keep them on hand for use only in emergencies.

Protection Systems

Determine needs for systems to detect abnormal situations, provide warning and protect property.

Consider:

- Fire protection systems
- Lightning protection systems
- Water-level monitoring systems
- Overflow detection devices
- Automatic shutoffs
- Emergency power generation systems

Consult your property insurer about special protective systems.

Mitigation

Consider ways to reduce the effects of emergencies, such as moving or constructing facilities away from flood plains and fault zones. Also consider ways to reduce the chances of emergencies from occurring, such as changing processes or materials used to run the business.

Consider physical retrofitting measures such as:

- Upgrading facilities to withstand the shaking of an earthquake or high winds
- "Floodproofing" facilities by constructing flood walls or other flood protection devices (see Section 3 for additional information)
- Installing fire sprinkler systems
- Installing fire-resistant materials and furnishing
- Installing storm shutters for all exterior windows and doors

There are also non-structural mitigation measures to consider, including:

- Installing fire-resistant materials and furnishing
- Securing light fixtures and other items that could fall or shake loose in an emergency
- Moving heavy or breakable objects to low shelves
- Attaching cabinets and files to low walls or bolting them together
- Placing Velcro strips under typewriters, tabletop computers and television monitors
- Moving work stations away from large windows
- Installing curtains or blinds that can be drawn over windows to prevent glass from shattering onto employees
- Anchoring water heaters and bolting them to wall studs

Consult a structural engineer or architect and your community's building and zoning offices for additional information.

Facility Shutdown

Facility shutdown is generally a last resort but always a possibility. Improper or disorganized shutdown can result in confusion, injury and property damage.

Some facilities require only simple actions such as turning off equipment, locking doors and activating alarms. Others require complex shutdown procedures.

Work with department heads to establish shutdown procedures. Include information about when and how to shut off utilities.

Identify:

- The conditions that could necessitate a shutdown
- Who can order a shutdown
- Who will carry out shutdown procedures
- How a partial shutdown would affect other facility operations
- The length of time required for shutdown and restarting

Train personnel in shutdown procedures. Post procedures.

Records Preservation

Vital records may include:

- Financial and insurance information
- Engineering plans and drawings
- Product lists and specifications
- Employee, customer and supplier databases
- Formulas and trade secrets
- Personnel files

Preserving vital records is essential to the quick restoration of operations. Analyzing vital records involves:

1. Classifying operations into functional categories, e.g., finance, production, sales, administration
2. Determining essential functions for keeping the business up and running, such as finance, production, sales, etc.
3. Identifying the minimum information that must be readily accessible to perform essential functions, e.g., maintaining customer collections may require access to account statements
4. Identifying the records that contain the essential information and where they are located
5. Identifying the equipment and materials needed to access and use the information

Next, establish procedures for protecting and accessing vital records. Among the many approaches to consider are:

- Labeling vital records
- Backing up computer systems
- Making copies of records
- Storing tapes and disks in insulated containers
- Storing data off-site where they would not likely be damaged by an event affecting your facility
- Increasing security of computer facilities
- Arranging for evacuation of records to backup facilities
- Backing up systems handled by service bureaus
- Arranging for backup power

Community Outreach

Your facility's relationship with the community will influence your ability to protect personnel and property and return to normal operations.

This section describes ways to involve outside organizations in the emergency management plan.

Involving the Community

Maintain a dialogue with community leaders, first responders, government agencies, community organizations and utilities, including:

- Appointed and elected leaders
- Fire, police and emergency medical services personnel
- Local Emergency Planning Committee (LEPC) members

- Emergency management director
- Public Works Department
- American Red Cross
- Hospitals
- Telephone company
- Electric utility
- Neighborhood groups

Have regular meetings with community emergency personnel to review emergency plans and procedures. Talk about what you're doing to prepare for and prevent emergencies. Explain your concern for the community's welfare.

Identify ways your facility could help the community in a community-wide emergency.

Look for common interests and concerns. Identify opportunities for sharing resources and information.

Conduct confidence-building activities such as facility tours. Do a facility walk-through with community response groups.

Involve community fire, police and emergency management personnel in drills and exercises.

Meet with your neighbors to determine how you could assist each other in an emergency.

Mutual Aid Agreements

To avoid confusion and conflict in an emergency, establish mutual aid agreements with local response agencies and businesses.

These agreements should:

- Define the type of assistance
- Identify the chain of command for activating the agreement
- Define communications procedures

Include these agencies in facility training exercises whenever possible.

Community Service

In community-wide emergencies, business and industry are often needed to assist the community with:

- Personnel
- Equipment
- Shelter
- Training
- Storage
- Feeding facilities
- EOC facilities

- Food, clothing, building materials
- Funding
- Transportation

While there is no way to predict what demands will be placed on your company's resources, give some thought to how the community's needs might influence your corporate responsibilities in an emergency. Also, consider the opportunities for community service before an emergency occurs.

Public Information

When site emergencies expand beyond the facility, the community will want to know the nature of the incident, whether the public's safety or health is in danger, what is being done to resolve the problem and what was done to prevent the situation from happening.

Determine the audiences that may be affected by an emergency and identify their information needs. Include:

- The public
- The media
- Employees and retirees
- Unions
- Contractors and suppliers
- Customers
- Shareholders
- Emergency response organizations
- Regulatory agencies
- Appointed and elected officials
- Special interest groups
- Neighbors

Media Relations

In an emergency, the media are the most important link to the public. Try to develop and maintain positive relations with media outlets in your area. Determine their particular needs and interests. Explain your plan for protecting personnel and preventing emergencies.

Determine how you would communicate important public information through the media in an emergency.

- Designate a trained spokesperson and an alternate spokesperson
- Set up a media briefing area
- Establish security procedures
- Establish procedures for ensuring that information is complete, accurate and approved for public release

- Determine an appropriate and useful way of communicating technical information
- Prepare background information about the facility

When providing information to the media during an emergency:

Do's

- Give all media equal access to information.
- When appropriate, conduct press briefings and interviews. Give local and national media equal time.
- Try to observe media deadlines.
- Escort media representatives to ensure safety.
- Keep records of information released.
- Provide press releases when possible.

Don'ts

- Do not speculate about the incident.
- Do not permit unauthorized personnel to release information.
- Do not cover up facts or mislead the media.
- Do not place blame for the incident.

Recovery and Restoration

Business recovery and restoration, or business resumption, goes right to a facility's bottom line: keeping people employed and the business running.

Planning Considerations

Consider making contractual arrangements with vendors for such post-emergency services as records preservation, equipment repair, earthmoving or engineering.

Meet with your insurance carriers to discuss your property and business resumptions policies (see the next page for guidelines).

Determine critical operations and make plans for bringing those systems back on-line. The process may entail:

- Repairing or replacing equipment
- Relocating operations to an alternate location
- Contracting operations on a temporary basis

Take photographs or videotape the facility to document company assets. Update these records regularly.

Continuity of Management

You can assume that not every key person will be readily available or physically at the facility after an emergency. Ensure that recovery decisions can be made without undue delay. Consult your legal department regarding laws and corporate bylaws governing continuity of management.

Establish procedures for:

- Assuring the chain of command
- Maintaining lines of succession for key personnel
- Moving to alternate headquarters

Include these considerations in all exercise scenarios.

Insurance

Most companies discover that they are not properly insured only after they have suffered a loss. Lack of appropriate insurance can be financially devastating. Discuss the following topics with your insurance advisor to determine your individual needs.

- How will my property be valued?
- Does my policy cover the cost of required upgrades to code?
- How much insurance am I required to carry to avoid becoming a co-insurer?
- What perils or causes of loss does my policy cover?
- What are my deductibles?
- What does my policy require me to do in the event of a loss?
- What types of records and documentation will my insurance company want to see? Are records in a safe place where they can be obtained after an emergency?
- To what extent am I covered for loss due to interruption of power? Is coverage provided for both on- and off-premises power interruption?
- Am I covered for lost income in the event of business interruption because of a loss? Do I have enough coverage? For how long is coverage provided? How long is my coverage for lost income if my business is closed by order of a civil authority?
- To what extent am I covered for reduced income due to customers' not all immediately coming back once the business reopens?
- How will my emergency management program affect my rates?

Employee Support

Since employees who will rely on you for support after an emergency are your most valuable asset, consider the range of services that you could provide or arrange for, including:

- Cash advances
- Salary continuation
- Flexible work hours
- Reduced work hours

- Crisis counseling
- Care packages
- Day care

Resuming Operations

Immediately after an emergency, take steps to resume operations.

- Establish a recovery team, if necessary. Establish priorities for resuming operations.
- Continue to ensure the safety of personnel on the property. Assess remaining hazards. Maintain security at the incident scene.
- Conduct an employee briefing.
- Keep detailed records. Consider audio recording all decisions. Take photographs of or video-tape the damage.
- Account for all damage-related costs. Establish special job order numbers and charge codes for purchases and repair work.
- Follow notification procedures. Notify employees' families about the status of personnel on the property. Notify off-duty personnel about work status. Notify insurance carriers and appropriate government agencies.
- Protect undamaged property. Close up building openings. Remove smoke, water and debris. Protect equipment against moisture. Restore sprinkler systems. Physically secure the property. Restore power.
- Conduct an investigation. Coordinate actions with appropriate government agencies.
- Conduct salvage operations. Segregate damaged from undamaged property. Keep damaged goods on hand until an insurance adjuster has visited the premises, but you can move material outside if it's seriously in the way and exposure to the elements won't make matters worse.
- Take an inventory of damaged goods. This is usually done with the adjuster, or the adjuster's salvor if there is any appreciable amount of goods or value. If you release goods to the salvor, obtain a signed inventory stating the quantity and type of goods being removed.
- Restore equipment and property. For major repair work, review restoration plans with the insurance adjuster and appropriate government agencies.
- Assess the value of damaged property. Assess the impact of business interruption.
- Maintain contact with customers and suppliers.

Administration and Logistics

Maintain complete and accurate records at all times to ensure a more efficient emergency response and recovery. Certain records may also be required by regulation or by your insurance carriers or prove invaluable in the case of legal action after an incident.

Administrative Actions

Administrative actions prior to an emergency include:

- Establishing a written emergency management plan
- Maintaining training records
- Maintaining all written communications
- Documenting drills and exercises and their critiques
- Involving community emergency response organizations in planning activities

Administrative actions during and after an emergency include:

- Maintaining telephone logs
- Keeping a detailed record of events
- Maintaining a record of injuries and follow-up actions
- Accounting for personnel
- Coordinating notification of family members
- Issuing press releases
- Maintaining sampling records
- Managing finances
- Coordinating personnel services
- Documenting incident investigations and recovery operations

Logistics

Before an emergency, logistics may entail:

- Acquiring equipment
- Stockpiling supplies
- Designating emergency facilities
- Establishing training facilities
- Establishing mutual aid agreements
- Preparing a resource inventory

During an emergency, logistics may entail the provision of:

- Providing utility maps to emergency responders
- Providing material safety data sheets to employees
- Moving backup equipment in place
- Repairing parts
- Arranging for medical support, food and transportation
- Arranging for shelter facilities
- Providing for backup power
- Providing for backup communications

SECTION 3: HAZARD-SPECIFIC INFORMATION

Fire

Fire is the most common of all the hazards. Every year fires cause thousands of deaths and injuries and billions of dollars in property damage.

Planning Considerations

Consider the following when developing your plan:

- Meet with the fire department to talk about the community's fire response capabilities. Talk about your operations. Identify processes and materials that could cause or fuel a fire, or contaminate the environment in a fire.
- Have your facility inspected for fire hazards. Ask about fire codes and regulations.
- Ask your insurance carrier to recommend fire prevention and protection measures. Your carrier may also offer training.
- Distribute fire safety information to employees: how to prevent fires in the workplace, how to contain a fire, how to evacuate the facility, where to report a fire.
- Instruct personnel to use the stairs—not elevators—in a fire. Instruct them to crawl on their hands and knees when escaping a hot or smoke-filled area.
- Conduct evacuation drills. Post maps of evacuation routes in prominent places. Keep evacuation routes including stairways and doorways clear of debris.
- Assign fire wardens for each area to monitor shutdown and evacuation procedures.
- Establish procedures for the safe handling and storage of flammable liquids and gases. Establish procedures to prevent the accumulation of combustible materials.
- Provide for the safe disposal of smoking materials.
- Establish a preventive maintenance schedule to keep equipment operating safely.
- Place fire extinguishers in appropriate locations.
- Train employees in use of fire extinguishers.
- Install smoke detectors. Check smoke detectors once a month, change batteries at least once a year.
- Establish a system for warning personnel of a fire. Consider installing a fire alarm with automatic notification to the fire department.
- Consider installing a sprinkler system, fire hoses and fire-resistant walls and doors.
- Ensure that key personnel are familiar with all fire safety systems.
- Identify and mark all utility shutoffs so that electrical power, gas or water can be shut off quickly by fire wardens or responding personnel.
- Determine the level of response your facility will take if a fire occurs. Among the options are:

Option 1—Immediate evacuation of all personnel on alarm.

Option 2—All personnel are trained in fire extinguisher use. Personnel in the immediate area of a fire attempt to control it. If they cannot, the fire alarm is sounded and all personnel evacuate.

Option 3—Only designated personnel are trained in fire extinguisher use.

Option 4—A fire team is trained to fight incipient-stage fires that can be controlled without protective equipment or breathing apparatus. Beyond this level fire, the team evacuates.

Option 5—A fire team is trained and equipped to fight structural fires using protective equipment and breathing apparatus.

Hazardous Materials Incidents

Hazardous materials are substances that are either flammable or combustible, explosive, toxic, noxious, corrosive, oxidizable, an irritant or radioactive.

A hazardous material spill or release can pose a risk to life, health or property. An incident can result in the evacuation of a few people, a section of a facility or an entire neighborhood.

There are a number of Federal laws that regulate hazardous materials, including: the Superfund Amendments and Reauthorization Act of 1986 (SARA), the Resource Conservation and Recovery Act of 1976 (RCRA), the Hazardous Materials Transportation Act (HMTA), the Occupational Safety and Health Act (OSHA), the Toxic Substances Control Act (TSCA) and the Clean Air Act.

Title III of SARA regulates the packaging, labeling, handling, storage and transportation of hazardous materials. The law requires facilities to furnish information about the quantities and health effects of materials used at the facility, and to promptly notify local and State officials whenever a significant release of hazardous materials occurs.

In addition to on-site hazards, you should be aware of the potential for an off-site incident affecting your operations. You should also be aware of hazardous materials used in facility processes and in the construction of the physical plant.

Detailed definitions as well as lists of hazardous materials can be obtained from the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA).

Planning Considerations

Consider the following when developing your plan:

- Identify and label all hazardous materials stored, handled, produced and disposed of by your facility. Follow government regulations that apply to your facility. Obtain material safety data sheets (MSDS) for all hazardous materials at your location.
- Ask the local fire department for assistance in developing appropriate response procedures.

- Train employees to recognize and report hazardous material spills and releases. Train employees in proper handling and storage.
- Establish a hazardous material response plan:
  - Establish procedures to notify management and emergency response organizations of an incident.
  - Establish procedures to warn employees of an incident.
  - Establish evacuation procedures.
  - Depending on your operations, organize and train an emergency response team to confine and control hazardous material spills in accordance with applicable regulations.
- Identify other facilities in your area that use hazardous materials. Determine whether an incident could affect your facility.
- Identify highways, railroads and waterways near your facility used for the transportation of hazardous materials. Determine how a transportation accident near your facility could affect your operations.

Floods and Flash Floods

Floods are the most common and widespread of all natural disasters. Most communities in the United States can experience some degree of flooding after spring rains, heavy thunderstorms or winter snow thaws.

Most floods develop slowly over a period of days. Flash floods, however, are like walls of water that develop in a matter of minutes. Flash floods can be caused by intense storms or dam failure.

Planning Considerations

Consider the following when preparing for floods:

- Ask your local emergency management office whether your facility is located in a flood plain. Learn the history of flooding in your area. Learn the elevation of your facility in relation to steams, rivers and dams.
- Review the community's emergency plan. Learn the community's evacuation routes. Know where to find higher ground in case of a flood.
- Establish warning and evacuation procedures for the facility. Make plans for assisting employees who may need transportation.
- Inspect areas in your facility subject to flooding. Identify records and equipment that can be moved to a higher location. Make plans to move records and equipment in case of flood.
- Purchase a NOAA Weather Radio with a warning alarm tone and battery backup. Listen for flood watches and warnings.

Flood Watch—Flooding is possible. Stay tuned to NOAA radio. Be prepared to evacuate. Tune to local radio and television stations for additional information.

Flood Warning—Flooding is already occurring or will occur soon. Take precautions at once. Be prepared to go to higher ground. If advised, evacuate immediately.

- Ask your insurance carrier for information about flood insurance. Regular property and casualty insurance does not cover flooding.
- Consider the feasibility of floodproofing your facility. There are three basic types of methods.
  1. Permanent floodproofing measures are taken before a flood occurs and require no human intervention when flood waters rise. They include:
     - Filling windows, doors or other openings with water-resistant materials such as concrete blocks or bricks. This approach assumes the structure is strong enough to withstand flood waters.
     - Installing check valves to prevent water from entering where utility and sewer lines enter the facility.
     - Reinforcing walls to resist water pressure. Sealing walls to prevent or reduce seepage.
     - Building watertight walls around equipment or work areas within the facility that are particularly susceptible to flood damage.
     - Constructing floodwalls or levees outside the facility to keep flood waters away.
     - Elevating the facility on walls, columns or compacted fill. This approach is most applicable to new construction, though many types of buildings can be elevated.
  2. Contingent floodproofing measures are also taken before a flood but require some additional action when flooding occurs. These measures include:
     - Installing watertight barriers called flood shields to prevent the passage of water through doors, windows, ventilation shafts or other openings
     - Installing permanent water-tight doors
     - Constructing movable floodwalls
     - Installing permanent pumps to remove flood waters
  3. Emergency floodproofing measures are generally less expensive than those listed above, though they require substantial advance warning and do not satisfy the minimum requirements for watertight floodproofing as set forth by the National Flood Insurance Program (NFIP). They include:
     - Building walls with sandbags
     - Constructing a double row of walls with boards and posts to create a "crib," then filling the crib with soil
     - Constructing a single wall by stacking small beams or planks on top of each other

- Consider the need for backup systems:
  - Portable pumps to remove flood water
  - Alternate power sources such as generators or gasoline-powered pumps

  - Battery-powered emergency lighting
- Participate in community flood control projects.

Hurricanes

Hurricanes are severe tropical storms with sustained winds of 74 miles per hour or greater. Hurricane winds can reach 160 miles per hour and extend inland for hundreds of miles.

Hurricanes bring torrential rains and a storm surge of ocean water that crashes into land as the storm approaches. Hurricanes also spawn tornadoes.

Hurricane advisories are issued by the National Weather Service as soon as a hurricane appears to be a threat. The hurricane season lasts from June through November.

Planning Considerations

The following are considerations when preparing for hurricanes:

- Ask your local emergency management office about community evacuation plans.
- Establish facility shutdown procedures. Establish warning and evacuation procedures. Make plans for assisting employees who may need transportation.
- Make plans for communicating with employees' families before and after a hurricane.
- Purchase a NOAA Weather Radio with a warning alarm tone and battery backup. Listen for hurricane watches and warnings.

Hurricane Watch—A hurricane is possible within 24 to 36 hours. Stay tuned for additional advisories. Tune to local radio and television stations for additional information. An evacuation may be necessary.

Hurricane Warning—A hurricane will hit land within 24 hours. Take precautions at once. If advised, evacuate immediately.

- Survey your facility. Make plans to protect outside equipment and structures.
- Make plans to protect windows. Permanent storm shutters offer the best protection. Covering windows with 5/8" marine plywood is a second option.
- Consider the need for backup systems:
  - Portable pumps to remove flood water
  - Alternate power sources such as generators or gasoline-powered pumps
  - Battery-powered emergency lighting
- Prepare to move records, computers and other items within your facility or to another location.

Tornadoes

Tornadoes are incredibly violent local storms that extend to the ground with whirling winds that can reach 300 mph.

Spawned from powerful thunderstorms, tornadoes can uproot trees and buildings and turn harmless objects into deadly missiles in a matter of seconds. Damage paths can be in excess of one mile wide and 50 miles long.

Tornadoes can occur in any state but occur more frequently in the Midwest, Southeast and Southwest. They occur with little or no warning.

Planning Considerations

The following are considerations when planning for tornadoes:

- Ask your local emergency management office about the community's tornado warning system.
- Purchase a NOAA Weather Radio with a warning alarm tone and battery backup. Listen for tornado watches and warnings.

Tornado Watch—Tornadoes are likely. Be ready to take shelter. Stay tuned to radio and television stations for additional information.

Tornado Warning—A tornado has been sighted in the area or is indicated by radar. Take shelter immediately.

- Establish procedures to inform personnel when tornado warnings are posted. Consider the need for spotters to be responsible for looking out for approaching storms.
- Work with a structural engineer or architect to designate shelter areas in your facility. Ask your local emergency management office or National Weather Service office for guidance.
- Consider the amount of space you will need. Adults require about six square feet of space; nursing home and hospital patients require more.
- The best protection in a tornado is usually an underground area. If an underground area is not available, consider:
    - Small interior rooms on the lowest floor and without windows
    - Hallways on the lowest floor away from doors and windows
    - Rooms constructed with reinforced concrete, brick or block with no windows and a heavy concrete floor or roof system overhead
    - Protected areas away from doors and windows

Note: Auditoriums, cafeterias and gymnasiums that are covered with a flat, wide-span roof are not considered safe.

- Make plans for evacuating personnel away from lightweight modular offices or mobile home-size buildings. These structures offer no protection from tornadoes.
- Conduct tornado drills.
- Once in the shelter, personnel should protect their heads with their arms and crouch down.

Severe Winter Storms

Severe winter storms bring heavy snow, ice, strong winds and freezing rain. Winter storms can prevent employees and customers from reaching the facility, leading to a temporary shutdown until roads are cleared. Heavy snow and ice can also cause structural damage and power outages.

Planning Considerations

Following are considerations for preparing for winter storms:

- Listen to NOAA Weather Radio and local radio and television stations for weather information:

  Winter Storm Watch—Severe winter weather is possible.

  Winter Storm Warning—Severe winter weather is expected.

  Blizzard Warning—Severe winter weather with sustained winds of at least 35 mph is expected.

  Traveler's Advisory—Severe winter conditions may make driving difficult or dangerous.
- Establish procedures for facility shutdown and early release of employees.
- Store food, water, blankets, battery-powered radios with extra batteries and other emergency supplies for employees who become stranded at the facility.
- Provide a backup power source for critical operations.
- Arrange for snow and ice removal from parking lots, walkways, loading docks, etc.

Earthquakes

Earthquakes occur most frequently west of the Rocky Mountains, although historically the most violent earthquakes have occurred in the central United States. Earthquakes occur suddenly and without warning.

Earthquakes can seriously damage buildings and their contents; disrupt gas, electric and telephone services; and trigger landslides, avalanches, flash floods, fires and huge ocean waves called tsunamis. Aftershocks can occur for weeks following an earthquake.

In many buildings, the greatest danger to people in an earthquake is when equipment and non-structural elements such as ceilings, partitions, windows and lighting fixtures shake loose.

Planning Considerations

Following are guidelines for preparing for earthquakes:

- Assess your facility's vulnerability to earthquakes. Ask local government agencies for seismic information for your area.

- Have your facility inspected by a structural engineer. Develop and prioritize strengthening measures. These may include:
  - Adding steel bracing to frames
  - Adding sheer walls to frames
  - Strengthening columns and building foundations
  - Replacing unreinforced brick filler walls
- Follow safety codes when constructing a facility or making major renovations.
- Inspect non-structural systems such as air conditioning, communications and pollution control systems. Assess the potential for damage. Prioritize measures to prevent damages.
- Inspect your facility for any item that could fall, spill, break or move during an earthquake. Take steps to reduce these hazards:
  - Move large and heavy objects to lower shelves or the floor. Hang heavy items away from where people work.
  - Secure shelves, filing cabinets, tall furniture, desktop equipment, computers, printers, copiers and light fixtures.
  - Secure fixed equipment and heavy machinery to the floor. Larger equipment can be placed on casters and attached to tethers which attach to the wall.
  - Add bracing to suspended ceilings, if necessary.
  - Install safety glass where appropriate.
  - Secure large utility and process piping.
- Keep copies of design drawings of the facility to be used in assessing the facility's safety after an earthquake.
- Review processes for handling and storing hazardous materials. Have incompatible chemicals stored separately.
- Ask your insurance carrier about earthquake insurance and mitigation techniques.
- Establish procedures to determine whether an evacuation is necessary after an earthquake.
- Designate areas in the facility away from exterior walls and windows where occupants should gather after an earthquake if an evacuation is not necessary.
- Conduct earthquake drills. Provide personnel with the following safety information:
  - In an earthquake, if indoors, stay there. Take cover under a sturdy piece of furniture or counter, or brace yourself against an inside wall. Protect your head and neck.
  - If outdoors, move into the open, away from buildings, street lights and utility wires.
  - After an earthquake, stay away from windows, skylights and items that could fall. Do not use the elevators.
  - Use stairways to leave the building if it is determined that a building evacuation is necessary.

Technological Emergencies

Technological emergencies include any interruption or loss of a utility service, power source, life support system, information system or equipment needed to keep the business in operation.

Planning Considerations

The following are suggestions for planning for technological emergencies:

- Identify all critical operations, including:
  - Utilities including electric power, gas, water, hydraulics, compressed air, municipal and internal sewer systems, wastewater treatment services
  - Security and alarm systems, elevators, lighting, life support systems, heating, ventilation and air conditioning systems, electrical distribution system
  - Manufacturing equipment, pollution control equipment
  - Communication systems, both data and voice computer networks
  - Transportation systems including air, highway, railroad and waterway
- Determine the impact of service disruption.
- Ensure that key safety and maintenance personnel are thoroughly familiar with all building systems.
- Establish procedures for restoring systems. Determine need for backup systems.
- Establish preventive maintenance schedules for all systems and equipment.

SECTION 4: INFORMATION SOURCES

Additional Readings from FEMA

The following publications can be obtained from FEMA by writing to: FEMA, Publications, P.O. Box 2012, Jessup, MD 20794-2012.

- Principal Threats Facing Communities and Local Emergency Management Coordinators (FEMA 191)—Statistics and analyses of natural disasters and man-made threats in the U.S.
- Floodproofing Non-Residential Structures (FEMA 102)—Technical information for building owners, designers and contractors on floodproofing techniques (200 pages).
- Non-Residential Floodproofing—Requirements and Certification for Buildings Located in Flood Hazard Areas in Accordance with the National Flood Insurance Program (FIA-TB-3)—Planning and engineering considerations for floodproofing new commercial buildings.
- Building Performance: Hurricane Andrew in Florida (FIA 22)—Technical guidance for enhancing the performance of buildings in hurricanes.

- Building Performance: Hurricane Iniki in Hawaii (FIA 23)—Technical guidance for reducing hurricane and flood damage.
- Answers to Questions About Substantially Damaged Buildings (FEMA 213)—Information about regulations and policies of the National Flood Insurance Program regarding substantially damaged buildings (25 pages).
- Design Guidelines for Flood Damage Reduction (FEMA 15)—A study on land use, watershed management, design and construction practices in floodprone areas.
- Comprehensive Earthquake Preparedness Planning Guidelines: Corporate (FEMA 71)—Earthquake planning guidance for corporate safety officers and managers.

Ready-to-Print Brochure Mechanicals for Your Employee Safety Program

You can provide your employees and customers with life-saving information from FEMA and the American Red Cross. Available at no charge is ready-to-print artwork for a series of brochures on disaster preparedness and family safety.

Select any of the brochures below, and you'll receive camera-ready materials, printing instructions and ideas for adding your own logo or sponsor message. Write to: Camera-ready Requests, Community & Family Preparedness Program, 500 C Street, SW Washington, DC 20472.

- Your Family Disaster Plan—A 4-step plan for individuals and families on how to prepare for any type of disaster.
- Emergency Preparedness Checklist—An action checklist on home safety, evacuation and disaster preparedness.
- Your Family Disaster Supplies Kit—A checklist of emergency supplies for the home and car.
- Helping Children Cope With Disaster—Practical advice on how to help children deal with the stress of disaster.

Emergency Management Offices

FEMA Headquarters

Federal Emergency
Management Agency, 500 C
Street, SW, Washington, DC
20472, (202)646-2500.

FEMA Regional Offices

- Region 1: Boston (617)223-9540
- Region 2: New York (212)225-7209

- Region 3: Philadelphia (215)931-5500
- Region 4: Atlanta (404)853-4200
- Region 5: Chicago (312)408-5500
- Region 6: Denton, TX (817)898-5104
- Region 7: Kansas City, MO (816)283-7061
- Region 8: Denver (303)235-1813
- Region 9: San Francisco (415)923-7100
- Region 10: Bothell, WA (206)487-4604

State Emergency Management Agencies

(FEMA region numbers are in parentheses.)

Alabama (4)
Alabama Emergency Management Agency
5898 S. County Rd. 41 Drawer 2160
Clanton, AL 35045-5160
(205)280-2201

Alaska (10)
Department of Military & Veteran Affairs
P.O. Box 5750
Camp Denali, AK 99595-5750
(907)428-7000

Arizona(9)
Arizona Division of Emergency Services
National Guard Bldg.
5636 E. McDowell Rd.
Phoenix, AZ 85008
(602)231-6245

Arkansas (6)
Office of Emergency Services
P.O. Box 758
Conway, AR 72032
(501)321-5601

California (9)
Office of Emergency Services
2800 Meadowview Rd.
Sacramento, CA 95823
(916)262-1816

Colorado (8)
Colorado Office of Emergency Management
Camp George West
Golden, CO 80401
(303)273-1622

Connecticut (1)
Connecticut Office of Emergency Management
360 Broad St.
Hartford, CT 06105
(203)566-3180

Delaware (3)
Division of Emergency Planning and Operations
P.O. Box 527
Delaware City, DE 19706
(302) 326-6000

District of Columbia (3)
Office of Emergency Preparedness
200 14th St., NW, 8th Floor
Washington, DC 20009
(202)727-3159

Florida (4)
Division of Emergency Management
2555 Shumar Oak Blvd.
Tallahassee, FL 32399-2100
(904)413-9969

Georgia (4)
Georgia Emergency Management Agency
P.O. Box 18055
Atlanta, GA 30316-0055
(404)635-7001

Hawaii (9)
State Civil Defense
3949 Diamond Head Rd.
Honolulu, HI 96816-4495
(808)733-4300

Idaho (10)
Bureau of Disaster Services
650 W. State St.
Boise, ID 83720
(208)334-2336

Illinois (5)
Illinois Emergency Management Agency
110 E. Adams St.
Springfield, IL 62706
(217)782-2700

Indiana (5)
Indiana Emergency Management Agency
State Office Bldg., Room E-208
302 W. Washington St.
Indianapolis, IN 46204
(317)232-3980

Iowa (7)
Iowa Emergency Management Division
Hoover State Office Bldg.
Level A, Room 29
Des Moines, IA 50319
(515)281-3231

Kansas (7)
Division of Emergency Preparedness
2800 S.W. Topeka Blvd
Topeka, KS 66611-1401
(913)274-1401

Kentucky (4)
Kentucky Disaster and Emergency Services
100 Minutemen Pkwy
Frankfort, KY 40601-6168
(502)564-8682

Louisiana (6)
Office of Emergency Preparedness
Department of Public Safety
LA Military Dept.
P.O. Box 44217
Capitol Station
Baton Rouge, LA 70804
(504)342-5470

Maine (1)
Maine Emergency Management Agency
72 State House Station
Augusta, ME 04333-0072
(207)287-4080

Maryland (3)
Maryland Emergency
Management and Civil Defense Agency
Two Sudbrook Ln., East
Pikesville, MD 21208
(410)486-4422

Massachusetts (1)
Massachusetts Emergency
Management Agency
P.O. Box 1496
Framingham, MA 01701-0317
(508)820-2000

Michigan (5)
Emergency Management Division
Michigan State Police
300 S. Washington Sq.
Suite 300
Lansing, MI 48913
(517)366-6198

Minnesota (5)
Division of Emergency Services
Department of Public Safety State Capitol,
B-5 St. Paul, MN 55155
(612)296-0450

Mississippi (4)
Mississippi Emergency
Management Agency
P.O. Box 4501, Fondren Station
Jackson, MS 39296
(601)352-9100

Missouri (7)
State Emergency Management Agency
P.O. Box 116
Jefferson City, MO 65102
(573)526-9101

Montana (8)
Emergency Management Specialist
Disaster and Emergency Services
P.O. Box 4789
Helena, MT 59604-4789
(406)444-6911

Nebraska
Nebraska Civil Defense Agency
National Guard Center
1300 Military Road
Lincoin, NE 68508-1090
(402)471-7410

Nevada (9)
Nevada Division of Emergency Services
2525 S. Carson St.
Carson City, NV 89710
(702)687-4240

New Hampshire (1)
Governor's Office of Emergency Management
State Office Park South
107 Pleasant St.
Concord, NH 03301-3809
(603)271-2231

New Jersey (2)
Office of Emergency Management
P.O. Box 7068
W. Trenton, NJ 08628-0068
(609)538-6050

New Mexico (6)
Emergency Planning and Coordination
Department of Public Safety
4491 Cerrillos Rd.
P.O. Box 1628
Santa Fe, NM 87504-1628
(505)827-9222

New York (2)
State Emergency Management Office
Bldg. #22, Suite 101
Albany, NY 12226-2251
(518)457-2222

North Carolina
Division of Emergency
Management
116 West Jones St.
Raleigh, NC 27603-1335
(919)733-5406

North Dakota (8)
North Dakota Division of Emergency Management
P.O. Box 5511
Bismarck, ND 58502-5511
(701)328-3300

Ohio (5)
Ohio Emergency Management Agency
2825 W. Dublin Granville Rd.
Columbus, OH 43235-2206
(614)889-7150

Oklahoma (6)
Oklahoma Civil Defense
P.O. Box 53365
Oklahoma City, OK 73152-3365
(405)521-2481

Oregon (10)
Emergency Management Division
Oregon State Executive Department
595 Cottage St., NE
Salem, OR 97310
(503)378-2911

Pennsylvania (3)
Pennsylvania Emergency
Management Agency
P.O. Box 3321
Harrisburg, PA 17105-3321
(717)651-2007

Puerto Rico (2)
State Civil Defense
Commonwealth of Puerto Rico
P.O. Box 5127
San Juan, PR 00906
(809)724-0124

Rhode Island (1)
Rhode Island Emergency Management Agency
675 New London Avenue
Cranston, RI 02920
(401)946-9996

South Carolina (4)
South Carolina Emergency
Management Division
1429 Senate St., Rutledge Bldg.
Columbia, SC 29201-3782
(803)734-8020

South Dakota (8)
Division of Emergency and Disaster Services
State Capitol, 500 East Capitol
Pierre, SD 57501
(605)773-3231

Tennessee (4)
Tennessee Emergency
Management Agency
3041 Sidco Dr. P.O. 41502
Nashville, TN 37204-1502
(615)741-6528

Texas (6)
Division of Emergency
Management
P.O. Box 4087
Austin, TX 78773-0001
(512)424-2000

Utah (8)
Division of Comprehensive Emergency Management
Sate Office Bldg., Room 1110
Salt Lake City, UT 84114
(801)538-3400

Vermont (1)
Vermont Emergency Management Agency
Dept. of Public Safety
Waterbury State Complex
103 S. Main St.
Waterbury, VT 05671-2101
(802)244-8271

Virgin Islands (2)
Territorial Emergency Management Agency
A & Q Building # 2c Estate Content
St Thomas, VI 00820
(809)773-2244

Virginia (3)
Department of Emergency Services
P.O. Box 40955
Richmond, VA 23225-6491
(804)674-2497

Washington (10)
Division of Emergency Management
4220 E. Martin Way, MS-PT 11
Olympia, WA 98504-0955
(360)923-4505

West Virginia (3)
West Virginia Office of Emergency Services
State Capitol Complex
Room EB80
Charleston, WV 25305-0360
(304)558-5380

Wisconsin (5)
Division of Emergency Government
2400 Wright St. P.O. Box 7865
Madison, WI 53707
(608)242-3232

Wyoming (8)
Wyoming Emergency Management Agency
P.O. Box 1709
Cheyenne, WY 82003
(307)777-7566

Vulnerability Analysis Chart

TYPE OF EMERGENCY	Probability	Human Impact	Property Impact	Business Impact	Internal Resources	External Resources	Total
	High Low 5 ↔ 1	High Impact 5 ↔ 1 Low Impact			Weak Resources 5 ↔ 1 Strong Resources		

The lower the score the better

Training Drills and Exercises

	January	February	March	April	May	June	July	August	September	October	November	December
MANAGEMENT ORIENTATION/REVIEW												
EMPLOYEE ORIENTATION/REVIEW												
CONTRACTOR ORIENTATION/REVIEW												
COMMUNITY/MEDIA ORIENTATION/REVIEW												
MANAGEMENT TABLETOP EXERCISE												
RESPONSE TEAM TABLETOP EXERCISE												
WALK-THROUGH DRILL												
FUNCTIONAL DRILLS												
EVACUATION DRILL												
FULL-SCALE EXERCISE												

READY BUSINESS: SAMPLE EMERGENCY PLAN

SAMPLE BUSINESS CONTINUITY AND DISASTER PREPAREDNESS PLAN

❐ PLAN TO STAY IN BUSINESS

Business Name

Address

City, State

Telephone Number

The following person is our primary crisis manager and will serve as the company spokesperson in an emergency.

Primary Emergency Contact

Telephone Number

Alternative Number

E-mail

❐ EMERGENCY CONTACT INFORMATION

Dial 9-1-1 in an Emergency

Non-Emergency Police/Fire

Insurance Provider

If this location is not accessible we will operate from location below:

Business Name

Address

City, State

Telephone Number

If the person is unable to manage the crisis, the person below will succeed in management:

Secondary Emergency Contact

Telephone Number

Alternative Number

E-mail

□ BE INFORMED

The following natural and man-made disasters could impact our business.

- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________

□ EMERGENCY PLANNING TEAM

The following people will participate in emergency planning and crisis management.

- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________

□ WE PLAN TO COORDINATE WITH OTHERS

The following people from neighboring businesses and our building management will participate on our emergency planning team.

- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________

□ OUR CRITICAL OPERATIONS

The following is a prioritized list of our critical operations, staff and procedures we need to recover from a disaster.

Operation	Staff in Charge	Action Plan
______________	______________	______________
______________	______________	______________
______________	______________	______________
______________	______________	______________
______________	______________	______________

❐ SUPPLIERS AND CONTRACTORS

Company Name: ____________________

Street Address: ____________________

City: __________ State: __________ Zip Code: __________

Phone: __________ Fax: __________ E-Mail: __________

Contact Name: __________ Account Number: __________

Materials/Service Provided: ____________________

If this company experiences a disaster, we will obtain supplies/materials from the following:

Company Name: ____________________

Street Address: ____________________

City: __________ State: __________ Zip Code: __________

Phone: __________ Fax: __________ E-Mail: __________

Contact Name: __________ Account Number: __________

Materials/Service Provided: ____________________

If this company experiences a disaster, we will obtain supplies/materials from the following:

Company Name: ____________________

Street Address: ____________________

City: __________ State: __________ Zip Code: __________

Phone: __________ Fax: __________ E-Mail: __________

Contact Name: __________ Account Number: __________

Materials/Service Provided: ____________________

❐ EVACUATION PLAN FOR ______________________ LOCATION

(Insert address)

- We have developed these plans in collaboration with neighboring businesses and building owners to avoid confusion or gridlock.
- We have located, copied and posted building and site maps.
- Exits are clearly marked.
- We will practice evacuation procedures _____________ times a year.

If we must leave the workplace quickly:

____

____

1. Warning System: ____

   We will test the warning system and record results _____________ times a year.

2. Assembly Site: ____

3. Assembly Site Manager & Alternate: ______________________________

   a. Responsibilities Include:

   ____

   ____

   ____

4. Shut Down Manager & Alternate: ________________________________

   a. Responsibilities Include:

   ____

   ____

   ____

5. ______________________ is responsible for issuing all clear.

□ SHELTER-IN-PLACE PLAN FOR ____________________ LOCATION

(Insert address)

- We have talked to co-workers about which emergency supplies, if any, the company will provide in the shelter location and which supplies individuals might consider keeping in a portable kit personalized for individual needs.
- We will practice shelter procedures ________________ times a year.

If we must take shelter quickly

____

____

1. Warning System: ____

   We will test the warning system and record results ________________ times a year.

2. Storm Shelter Location: ____

3. "Seal the Room" Shelter Location: ____________________________________

4. Shelter Manager & Alternate:

   a. Responsibilities Include:

   ____

   ____

   ____

5. Shut Down Manager & Alternate: _______________________________________

   a. Responsibilities Include:

   ____

   ____

   ____

6. ____________________________ is responsible for issuing all clear.

□ COMMUNICATIONS

We will communicate our emergency plans with co-workers in the following way:

____

____

In the event of a disaster we will communicate with employees in the following way:

____

____

□ CYBER SECURITY

To protect our computer hardware, we will:

____

To protect our computer software, we will:

____

If our computers are destroyed, we will use back-up computers at the following location:

____

□ RECORDS BACK-UP

____________________________ is responsible for backing up our critical records including payroll and accounting systems.

Back-up records including a copy of this plan, site maps, insurance policies, bank account records and computer back ups are stored onsite ____________________________

Another set of back-up records is stored at the following off-site location:

____

If our accounting and payroll records are destroyed, we will provide for continuity in the following ways:

____

□ EMPLOYEE EMERGENCY CONTACT INFORMATION

The following is a list of our co-workers and their individual emergency contact information:

____________________ ____________________ ____________________

____________________ ____________________ ____________________

____________________ ____________________ ____________________

____________________ ____________________ ____________________

□ ANNUAL REVIEW

We will review and update this business continuity and disaster plan in __________.

FEMA: PROTECTING YOUR BUSINESS FROM DISASTERS

ARE YOU AT RISK?

If you aren't sure whether your business is at risk from disasters caused by natural hazards, check with your local building official, city engineer, or planning and zoning administrator. They can tell you whether you are in an area where hurricanes, floods, earthquakes, wildfires, or tornadoes are likely to occur. Also, they usually can tell you how to protect your business.

WHAT YOU CAN DO

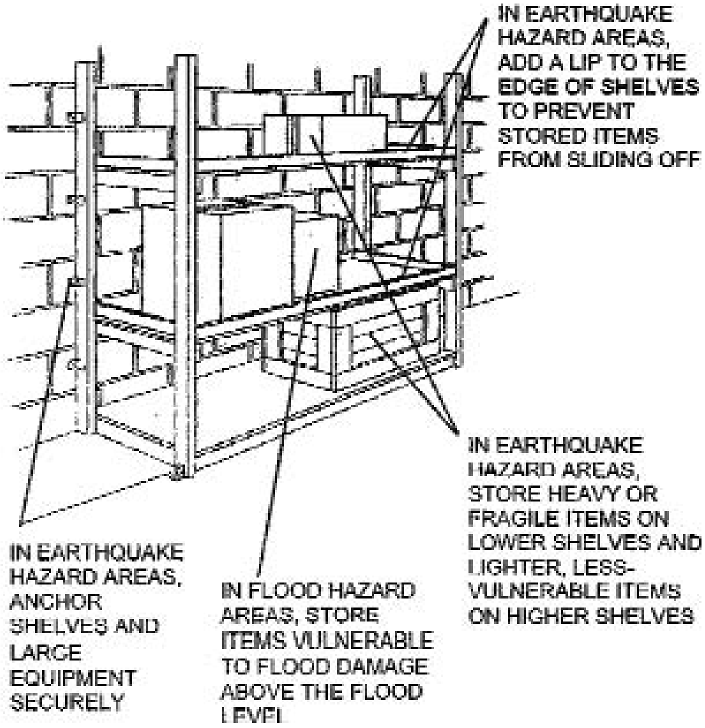
Protecting your business from disasters caused by natural hazards can involve a variety of actions, from inspecting and maintaining your buildings to installing protective devices. Most of these actions, especially those that affect the structure of your buildings or their utility systems, should be carried out by qualified maintenance staff or professional contractors licensed to work in your state, country, or city. One example of disaster protection is safely storing the important documents, electronic files, raw materials, and inventory required for the operation of your business.

PROTECT BUSINESS RECORDS AND INVENTORY

Most businesses keep on-site records and files (both hardcopy and electronic) that are essential to normal operations. Some businesses also store raw materials and product inventory. The loss of essential records, files, and other materials during a disaster is commonplace and can not only add to your damage costs, but also delay your return to normal operations. The longer your business is not operating, the more likely you are to lose customers permanently to your competitors.

To reduce your vulnerability, determine which records, files, and materials are most important; consider their vulnerability to damage during different types of disasters (such as floods, hurricanes, and earthquakes); and take steps to protect them, including the following:

- raising computers above the flood level and moving them away from large windows
- moving heavy and fragile objects to low shelves
- storing vital documents (plans, legal papers, etc.) in a secure off-site location
- regularly backing up vital electronic files (such as billing and payroll records and customer lists) and storing backup copies in a secure off-site location
- securing equipment that could move or fall during an earthquake.


IN EARTHQUAKE HAZARD AREAS, ADD A LIP TO THE EDGE OF SHELVES TO PREVENT STORED ITEMS FROM SLIDING OFF
IN EARTHQUAKE HAZARD AREAS, STORE HEAVY OR FRAGILE ITEMS ON LOWER SHELVES AND LIGHTER, LESS-VULNERABLE ITEMS ON HIGHER SHELVES
IN EARTHQUAKE HAZARD AREAS, ANCHOR SHELVES AND LARGE EQUIPMENT SECURELY
IN FLOOD HAZARD AREAS, STORE ITEMS VULNERABLE TO FLOOD DAMAGE ABOVE THE FLOOD LEVEL

TIPS

Keep these points in mind when you protect business records and inventory:

- Make sure you are aware of the details of your flood insurance and other hazard insurance policies, specifically which items and contents are covered and under what conditions. For example, if you have a home business, you may need two flood insurance policies, a home policy and a separate business policy, depending on the percentage of the total square footage of your house that is devoted to business use. Check with your insurance agent if you have questions about any of your policies.
- When you identify equipment susceptible to damage, consider the location of the equipment. For example, equipment near a hot water tank or pipes could be damaged if the pipes burst during an earthquake, and equipment near large windows could be damaged during hurricanes.
- Assign disaster mitigation duties to your employees. For example, some employees could be responsible for securing storage bins and others for backing up computer files and delivering copies to a secure location.
- You may want to consider having other offices of your company, or a contractor, perform some administrative duties, such as maintaining payroll records or providing customer service.
- Estimate the cost of repairing or replacing each essential piece of equipment in your business. Your estimates will help you assess your vulnerability and focus your efforts.
- For both insurance and tax purposes, you should maintain written and photographic inventories of all important materials and equipment. The inventory should be stored in a safety deposit box or other secure location.

ESTIMATED COST

The cost of these measures will depend on the size and contents of your business, the nature of the potential hazards, and the effort required to ensure proper protection. In some instances, you may need to buy new equipment, such as a backup tape drive system.

OTHER SOURCES OF INFORMATION

Emergency Management Guide for Business & Industry, FEMA, 1996.
Separate Flood Insurance a Must, FEMA, 1996.
To obtain copies of FEMA documents, call FEMA Publications at 1-800-480-2520. Information is also available on the World Wide Web at http//:www.fema.gov.

GUIDANCE ON PREPARING WORKPLACES FOR AN INFLUENZA PANDEMIC

U.S. Department of Labor, Occupational Safety and Health Administration

INTRODUCTION

A pandemic is a global disease outbreak. An influenza pandemic occurs when a new influenza virus emerges for which there is little or no immunity in the human population, begins to cause serious illness and then spreads easily person-to-person worldwide. A worldwide influenza pandemic could have a major effect on the global economy, including travel, trade, tourism, food, consumption and eventually, investment and financial markets. Planning for pandemic influenza by business and industry is essential to minimize a pandemic's impact. Companies that provide critical infrastructure services, such as power and telecommunications, also have a special responsibility to plan for continued operation in a crisis and should plan accordingly. As with any catastrophe, having a contingency plan is essential.

In the event of an influenza pandemic, employers will play a key role in protecting employees' health and safety as well as in limiting the impact on the economy and society. Employers will likely experience employee absences, changes in patterns of commerce and interrupted supply and delivery schedules. Proper planning will allow employers in the public and private sectors to better protect their employees and lessen the impact of a pandemic on society and the economy. As stated in the President's *National Strategy for Pandemic Influenza*, all stakeholders must plan and be prepared.

The Occupational Safety and Health Administration (OSHA) developed this pandemic influenza planning guidance based upon traditional infection control and industrial hygiene practices. It is important to note that there is currently no pandemic; thus, this guidance is intended for planning purposes and is not specific to a particular viral strain. Additional guidance may be needed as an actual pandemic unfolds and more is known about the characteristics of the virulence of the virus, disease transmissibility, clinical manifestation, drug susceptibility, and risks to different age groups and subpopulations. Employers and employees should use this planning guidance to help identify risk levels in

This guidance is advisory in nature and informational in content. It is not a standard or a regulation, and it neither creates new legal obligations nor alters existing obligations created by OSHA standards or the *Occupational Safety and Health Act* (OSH Act). Pursuant to the OSH Act, employers must comply with hazard-specific safety and health standards as issued and enforced either by OSHA or by an OSHA approved State Plan. In addition, Section 5(a)(1) of the OSH Act, the General Duty Clause, requires employers to provide their employers with a workplace free from recognized hazards likely to cause death or serious physical harm. Employers can be cited for violating the General Duty Clause if there is a recognized hazard and they do not take reasonable steps to prevent or abate the hazard. However, failure to implement any recommendations in this guidance is not, in itself, a violation of the General Duty Clause. Citations can only be based on standards, regulations, or the General Duty Clause.

workplace settings and appropriate control measures that include good hygiene, cough etiquette, social distancing, the use of personal protective equipment, and staying home from work when ill. Up-to-date information and guidance is available to the public through the www.pandemicflu.gov website.

THE DIFFERENCE BETWEEN SEASONAL, PANDEMIC INFLUENZA AND AVIAN INFLUENZA

Seasonal influenza refers to the periodic outbreaks of respiratory illness in the fall and winter in the United States. Outbreaks are typically limited; most people have some immunity to the circulating strain of the virus. A vaccine is prepared in advance of the seasonal influenza; it is designed to match the influenza viruses most likely to be circulating in the community. Employees living abroad and international business travelers should note that other geographic areas (for example, the Southern Hemisphere) have different influenza seasons which may require different vaccines.

Pandemic influenza refers to a worldwide outbreak of influenza among people when a new strain of the virus emerges that has the ability to infect humans and to spread from person to person. During the early phases of an influenza pandemic, people might not have any natural Immunity to the new strain; so the disease would spread rapidly among the population. A vaccine to protect people against illness from a pandemic influenza virus may not be widely available until many months after an influenza pandemic begins. It is important to emphasize that there currently is no influenza pandemic. However, pandemics have occurred throughout history and many scientists believe that it is only a matter of time before another one occurs. Pandemics can vary in severity from something that seems simply like a bad flu season to an especially severe influenza pandemic that could lead to high levels of illness, death, social disruption and economic loss. It is Impossible to predict when the next pandemic will occur or whether it will be mild or severe.

Avian influenza (AI)—also known as the bird flu—is caused by virus that infects wild birds and domestic poultry. Some forms of the avian influenza are worse than others. Avian influenza viruses are generally divided into two groups: low pathogenic avian influenza and highly pathogenic avian influenza. Low pathogenic avian influenza naturally occurs in wild birds and can spread to domestic birds. In most cases, it causes no signs of infection or only minor symptoms in birds. In general, these low path strains of the virus pose little threat to human health. Low pathogenic avian influenza virus H5 and H7 strains have the potential to mutate into highly pathogenic avian influenza and are, therefore, closely monitored. Highly pathogenic avian influenza spreads rapidly and has a high death rate in birds. Highly pathogenic avian influenza of the H5N1 strain is rapidly spreading in birds in some parts of the world.

Highly pathogenic H5N1 is one of the few avian influenza viruses to have crossed the species barrier to infect humans and it is the most deadly of those that have crossed the barrier. Most cases of H5N1 influenza infection in humans have resulted from contact with infected poultry or surfaces contaminated with secretions/excretions from infected birds.

As of February 2007, the spread of H5N1 virus from person to person has been limited to rare, sporadic cases. Nonetheless, because all influenza viruses have the ability to change, scientists are concerned that H5N1 virus one day could be able to sustain human to human transmission. Because these viruses do not commonly infect humans, there is little or no immune protection against them in the human population. If H5N1 virus were to gain the capacity to sustain transmission from person to person, a pandemic could begin.

An update on what is currently known about avian flu can be found at www.pandemicflu.gov.

HOW A SEVERE PANDEMIC INFLUENZA COULD AFFECT WORKPLACES

Unlike natural disasters or terrorist events, an influenza pandemic will be widespread, affecting multiple areas of the United States and other countries at the same time. A pandemic will also be an extended event, with multiple waves of outbreaks in the same geographic area; each outbreak could last from 6 to 8 weeks. Waves of outbreaks may occur over a year or more. Your workplace will likely experience:

- *Absenteeism*—A pandemic could affect as many as 40 percent of the workforce during periods of peak influenza illness. Employees could be absent because they are sick, must care for sick family members or for children if schools or day care centers are closed, are afraid to come to work, or the employer might not be notified that the employee has died.
- *Change in patterns of commerce*—During a pandemic, consumer demand for items related to infection control is likely to increase dramatically, while consumer interest in other goods may decline. Consumers may also change the ways in which they shop as a result of the pandemic. Consumers may try to shop at off-peak hours to reduce contact with other people, show increased interest in home delivery services, or prefer other options, such as drive-through service, to reduce person-to-person contact.
- *Interrupted supply/delivery*—Shipments of items from those geographic areas severely affected by the pandemic may be delayed or cancelled.

WHO SHOULD PLAN FOR A PANDEMIC

To reduce the impact of a pandemic on your operations, employees, customers and the general public, it is important for all businesses and organizations to begin continuity planning for a pandemic now. Lack of continuity planning can result in a cascade of failures as employers attempt to address challenges of a pandemic with insufficient resources and employees who might not be adequately trained in the jobs they will be asked to perform. Proper planning will allow employers to better protect their employees and prepare for changing patterns of commerce and potential disruptions in supplies or services. Important tools for pandemic planning for employers are located at www.pandemicflu.gov.

The U.S. government has placed a special emphasis on supporting pandemic influenza planning for public and private sector businesses deemed to be critical industries and key resources (Cl/KR). Critical infrastructure are the thirteen sectors that provide the production of essential goods and services, interconnectedness and operability, public safety, and security that contribute to a strong national defense and thriving economy. Key resources are facilities, sites, and groups of organized people whose destruction could cause large-scale injury, death, or destruction of property and/or profoundly damage our national prestige and confidence. With 85 percent of the nation's critical infrastructure in the hands of the private sector, the business community plays a vital role in ensuring national pandemic preparedness and response. Additional guidance for CI/KR business is available at: www.pandemicflu.gov/plan/pdf/CIKRpandemicInfluenzaGuide.pdf.

Critical Infrastructure and Key Resources

Key Resources

- Government Facilities
- Dams
- Commercial Facilities
- Nuclear Power Plants

Critical Infrastructure

- Food and Agriculture
- Public Health and Healthcare
- Banking and Finance
- Chemical and Hazardous Materials
- Defense Industrial Base
- Water
- Energy
- Emergency Services
- Information Technology
- Telecommunications
- Postal and Shipping
- Transportation
- National Monuments and Icons

HOW INFLUENZA CAN SPREAD BETWEEN PEOPLE

Influenza is thought to be primarily spread through large droplets (droplet transmission) that directly contact the nose, mouth or eyes. These droplets are produced when infected people cough, sneeze or talk, sending the relatively large infectious droplets and very small sprays (aerosols) into the nearby air and into contact with other people. Large droplets can only travel a limited range; therefore, people should limit close contact (within 6 feet) with others when possible. To a lesser degree, human influenza is spread by touching objects contaminated with influenza viruses and then transferring the infected material from the hands to the nose, mouth or eyes. Influenza may also be spread by very small infectious particles (aerosols) traveling in the air. The contribution of each route of exposure to influenza transmission is uncertain at this time and may vary based upon the characteristics of the influenza strain.

CLASSIFYING EMPLOYEE EXPOSURE TO PANDEMIC INFLUENZA AT WORK

Employee risks of occupational exposure to influenza during a pandemic may vary from very high to high, medium, or lower (caution) risk. The level of risk depends in part on whether or not jobs require close proximity to people potentially infected with the pandemic influenza virus, or whether they are required to have either repeated or extended contact with known or suspected sources of pandemic influenza virus such as coworkers, the general public, outpatients, school children or other such individuals or groups.

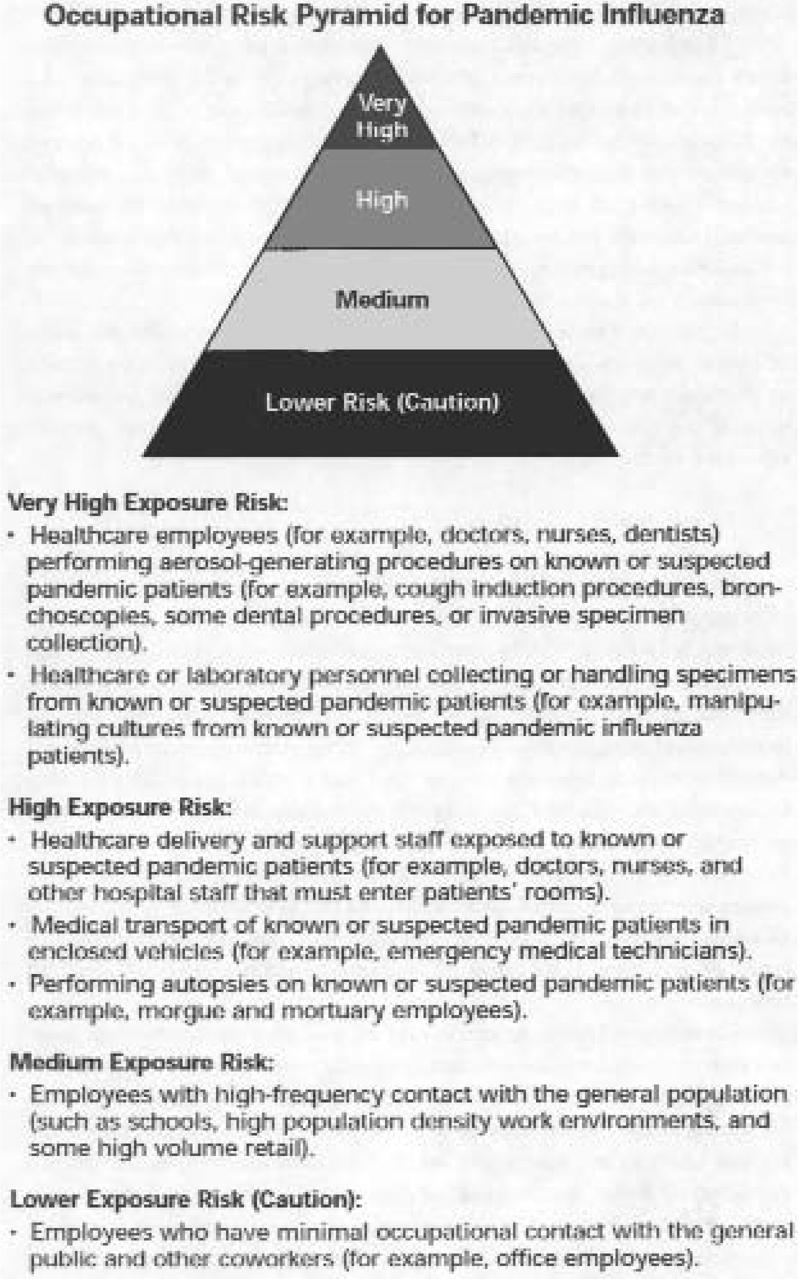
- *Very high exposure risk* occupations are those with high potential exposure to high concentrations of known or suspected sources of pandemic influenza during specific medical or laboratory procedures.
- *High exposure risk* occupations are those with high potential for exposure to known or suspected sources of pandemic influenza virus.
- *Medium exposure risk* occupations include jobs that require frequent, close contact (within 6 feet) exposures to known or suspected sources of pandemic influenza virus such as coworkers, the general public, outpatients, school children or other such individuals or groups.
- *Lower exposure risk (caution)* occupations are those that do not require contact with people known to be infected with the pandemic virus, nor frequent close contact (within 6 feet) with the public. Even at lower risk levels, however, employers should be cautious and develop preparedness plans to minimize employee infections.

Employers of critical infrastructure and key resource employees (such as law enforcement, emergency response, or public utility employees) may consider upgrading protective measures for these employees beyond what would be suggested by their exposure risk due to the necessity of such services for the functioning of society as well as the potential difficulties in replacing them during a pandemic (for example, due to extensive training or licensing requirements).

To help employers determine appropriate work practices and precautions, OSHA has divided workplaces and work operations into four risk zones, according to the likelihood of employees' occupational exposure to pandemic influenza. We show these zones in the shape of a pyramid to represent how the risk will likely be distributed (see page 11). The vast majority of American workplaces are likely to be in the medium exposure risk or lower exposure risk (caution) groups.

HOW TO MAINTAIN OPERATIONS DURING A PANDEMIC

As an employer, you have an important role in protecting employee health and safety, and limiting the impact of an influenza pandemic. It is important to work with community planners to integrate your pandemic plan into local and state planning, particularly if your operations are part of the nation's critical infrastructure or key resources. Integration with local community planners will allow you to access resources and information promptly to maintain operations and keep your employees safe.



Occupational Risk Pyramid for Pandemic Influenza

Very High
High
Medium
Lower Risk (Caution)

Very High Exposure Risk:

- Healthcare employees (for example, doctors, nurses, dentists) performing aerosol-generating procedures on known or suspected pandemic patients (for example, cough induction procedures, bronchoscopies, some dental procedures, or invasive specimen collection).
- Healthcare or laboratory personnel collecting or handling specimens from known or suspected pandemic patients (for example, manipulating cultures from known or suspected pandemic influenza patients).

High Exposure Risk:

- Healthcare delivery and support staff exposed to known or suspected pandemic patients (for example, doctors, nurses, and other hospital staff that must enter patients' rooms).
- Medical transport of known or suspected pandemic patients in enclosed vehicles (for example, emergency medical technicians).
- Performing autopsies on known or suspected pandemic patients (for example, morgue and mortuary employees).

Medium Exposure Risk:

- Employees with high-frequency contact with the general population (such as schools, high population density work environments, and some high volume retail).

Lower Exposure Risk (Caution):

- Employees who have minimal occupational contact with the general public and other coworkers (for example, office employees).

Develop a Disaster Plan

Develop a disaster plan that includes pandemic preparedness (See www.pandemicflu.gov/plan/businesschecklist.html) and review it and conduct drills regularly.

- Be aware of and review federal, state and local health department pandemic influenza plans. Incorporate appropriate actions from these plans into workplace disaster plans.
- Prepare and plan for operations with a reduced workforce.
- Work with your suppliers to ensure that you can continue to operate and provide services.
- Develop a sick leave policy that does not penalize sick employees, thereby encouraging employees who have influenza-related symptoms (e.g., fever, headache, cough, sore throat, runny or stuffy nose, muscle aches, or upset stomach) to stay home so that they do not infect other employees. Recognize that employees with ill family members may need to stay home to care for them.
- Identify possible exposure and health risks to your employees. Are employees potentially in contact with people with influenza such as in a hospital or clinic? Are your employees expected to have a lot of contact with the general public?
- Minimize exposure to fellow employees or the public. For example, will more of your employees work from home? This may require enhancement of technology and communications equipment.
- Identify business-essential positions and people required to sustain business-necessary functions and operations. Prepare to cross-train or develop ways to function in the absence of these positions. It is recommended that employers train three or more employees to be able to sustain business-necessary functions and operations, and communicate the expectation for available employees to perform these functions if needed during a pandemic.
- Plan for downsizing services but also anticipate any scenario which may require a surge in your services.
- Recognize that, in the course of normal daily life, all employees will have non-occupational risk factors at home and in community settings that should be reduced to the extent possible. Some employees will also have individual risk factors that should be considered by employers as they plan how the organization will respond to a potential pandemic (e.g., Immuno-compromised individuals and pregnant women).
- Stockpile items such as soap, tissue, hand sanitizer, cleaning supplies and recommended personal protective equipment. When stockpiling items, be aware of each product's shelf life and storage conditions (e.g., avoid areas that are damp or have temperature extremes) and incorporate product rotation (e.g., consume oldest supplies first) into your stockpile management program.

Make sure that your disaster plan protects and supports your employees, customers and the general public. Be aware of your employees' concerns about pay, leave, safety and health. Informed employees who feel safe at work are less likely to be absent.

- Develop policies and practices that distance employees from each other, customers and the general public. Consider practices to minimize face-to-face contact between employees such as e-mail, websites and teleconferences. Policies and practices that allow employees to work from home or to stagger their work shifts may be important as absenteeism rises.
- Organize and identify a central team of people or focal point to serve as a communication source so that your employees and customers can have accurate information during the crisis.
- Work with your employees and their union(s) to address leave, pay, transportation, travel, childcare, absence and other human resource issues.
- Provide your employees and customers in your workplace with easy access to infection control supplies, such as soap, hand sanitizers, personal protective equipment (such as gloves or surgical masks), tissues, and office cleaning supplies.
- Provide training, education and informational material about business-essential job functions and employees health and safety, including proper hygiene practices and the use of any personal protective equipment to be used in the workplace. Be sure that informational material is available in a usable format for individuals with sensory disabilities and/or limited English proficiency. Encourage employees to take care of their health by eating right, getting plenty of rest and getting a seasonal flu vaccination.
- Work with your insurance companies, and state and local health agencies to provide information to employees and customers about medical care in the event of a pandemic.
- Assist employees in managing additional stressors related to the pandemic. These are likely to include distress related to personal or family illness, life disruption, grief related to loss of family, friends or coworkers, loss of routine support systems, and similar challenges. Assuring timely and accurate communication will also be important throughout the duration of the pandemic in decreasing fear or worry. Employers should provide opportunities for support, counseling, and mental health assessment and referral should these be necessary. If present, Employee Assistance Programs can offer training and provide resources and other guidance on mental health and resiliency before and during a pandemic.

Protect Employees and Customers

Educate and train employees in proper hand hygiene, cough etiquette and social distancing techniques. Understand and develop work practice and engineering controls that could provide additional protection to your employees and customers, such as: drive-through service windows, clear plastic sneeze barriers, ventilation, and the proper selection, use and disposal of personal protective equipment.

These are not comprehensive recommendations. The most important part of pandemic planning is to work with your employees, local and state agencies and other employers to develop cooperative pandemic plans to maintain your operations and keep your employees and the public safe. Share what you know, be open to ideas from your employees, then identify and share effective health practices with other employers in your community and with your local chamber of commerce.

HOW ORGANIZATIONS CAN PROTECT THEIR EMPLOYEES

For most employers, protecting their employees will depend on emphasizing proper hygiene (disinfecting hands and surfaces) and practicing social distancing (see page 26 for more information). Social distancing means reducing the frequency, proximity, and duration of contact between people (both employees and customers) to reduce the chances of spreading pandemic influenza from person-to-person. All employers should implement good hygiene and infection control practices.

Occupational safety and health professionals use a framework called the "hierarchy of controls" to select ways of dealing with workplace hazards. The hierarchy of controls prioritizes intervention strategies based on the premise that the best way to control a hazard is to systematically remove it from the workplace, rather than relying on employees to reduce their exposure. In the setting of a pandemic, this hierarchy should be used in concert with current public health recommendations. The types of measures that may be used to protect yourself, your employees, and your customers (listed from most effective to least effective) are: engineering controls, administrative controls, work practices, and personal protective equipment (PPE). Most employers will use a combination of control methods. There are advantages and disadvantages to each type of control measure when considering the ease of implementation, effectiveness, and cost. For example, hygiene and social distancing can be implemented relatively easily and with little expense, but this control method requires employees to modify and maintain their behavior, which may be difficult to sustain. On the other hand, installing clear plastic barriers or a drive-through window will be more expensive and take a longer time to implement, although in the long run may be more effective at preventing transmission during a pandemic. Employers must evaluate their particular workplace to develop a plan for protecting their employees that may combine both immediate actions as well as longer term solutions.

Here is a description of each type of control:

Work Practice and Engineering Controls—Historically, infection control professionals have relied on personal protective equipment (for example, surgical masks and gloves) to serve as a physical barrier in order to prevent the transmission of an infectious disease from one person to another. This reflects the fact that close interactions with infectious patients is an unavoidable part of many healthcare occupations. The principles of industrial hygiene demonstrate that work practice controls and engineering controls can also serve as barriers to transmission and are less reliant on employee behavior to provide protection. Work practice controls are procedures for safe and proper work that are used to reduce the duration, frequency or intensity of exposure to a hazard. When defining safe work practice controls, it is a good idea to ask your employees for their suggestions, since they have firsthand experience with the tasks. These controls should be understood and followed by managers, supervisors and employees. When work practice controls are insufficient to protect employees, some employers may also need engineering controls.

Engineering controls involve making changes to the work environment to reduce work-related hazards. These types of controls are preferred over all others because they make permanent changes that reduce exposure to hazards and do not rely on employee or customer behavior. By reducing a hazard in the workplace, engineering controls can be the most cost-effective solutions for employers to implement.

During a pandemic, engineering controls may be effective in reducing exposure to some sources of pandemic influenza and not others. For example, installing sneeze guards between customers and employees would provide a barrier to transmission. The use of barrier protections, such as sneeze guards, is common practice for both infection control and industrial hygiene. However, while the installation of sneeze guards may reduce or prevent transmission between customers and employees, transmission may still occur between coworkers. Therefore, administrative controls and public health measures should be implemented along with engineering controls.

Examples of work practice controls include:

- Providing resources and a work environment that promotes personal hygiene. For example, provide tissues, no-touch trash cans, hand soap, hand sanitizer, disinfectants and disposable towels for employees to clean their work surfaces.
- Encouraging employees to obtain a seasonal influenza vaccine (this helps to prevent illness from seasonal influenza strains that may continue to circulate).
- Providing employees with up-to-date education and training on influenza risk factors, protective behaviors, and instruction on proper behaviors (for example, cough ettiquette and care of personal protective equipment).
- Developing policies to minimize contacts between employees and between employees and clients or customers.

More information about protecting yourself, your coworkers and employees, and your family can be found at www.pandemicflu.gov.

Examples of engineering controls include:

- Installing physical barriers, such as clear plastic sneeze guards.
- Installing a drive-through window for customer service.
- In some limited healthcare settings, for aerosol generating procedures, specialized negative pressure ventilation may be indicated.

Administrative Controls—Administrative controls include controlling employees' exposure by scheduling their work tasks in ways that minimize their exposure levels. Examples of administrative controls include:

- Developing policies that encourage ill employees to stay at home without fear of any reprisals.
- The discontinuation of unessential travel to locations with high illness transmission rates.
- Consider practices to minimize face-to-face contact between employees such as e-mail, websites and teleconferences. Where possible, encourage flexible work arrangements such as telecommuting or flexible work hours to reduce the number of your employees who must be at work at one time or in one specific location.
- Consider home delivery of goods and services to reduce the number of clients or customers who must visit your workplace.
- Developing emergency communications plans. Maintain a forum for answering employees' concerns. Develop internet-based communications if feasible.

Personal Protective Equipment (PPE)—While administrative and engineering controls and proper work practices are considered to be more effective in minimizing exposure to the influenza virus, the use of PPE may also be indicated during certain exposures. If used correctly, PPE can help prevent some exposures; however, they should not take the place of other prevention interventions, such as engineering controls, cough etiquette, and hand hygiene (see www.cdc.gov/flu/protect/stopgerms.htm). Examples of personal protective equipment are gloves, goggles, face shields, surgical masks, and respirators (for example, N-95). It is important that personal protective equipment be:

- Selected based upon the hazard to the employee;
- Properly fitted and some must be periodically refitted (e.g., respirators);
- Conscientiously and properly worn;
- Regularly maintained and replaced, as necessary;
- Properly removed and disposed of to avoid contamination of self, others or the environment.

Employers are obligated to provide their employees with protective gear needed to keep them safe while performing their jobs. The types of PPE recommended for pandemic influenza will be based on the risk of contracting influenza while working and the availability of PPE. Check the www.pandemicflu.gov website for the latest guidance.

THE DIFFERENCE BETWEEN A SURGICAL MASK AND A RESPIRATOR

It is important that employers and employees understand the significant differences between these types of personal protective equipment. The decision on whether or not to require employees to use either surgical/procedure masks or respirators must be based upon a hazard analysis of the employees' specific work environment and the differing protective properties of each type of personal protective equipment. The use of surgical masks or respirators is one component of infection control practices that may reduce transmission between infected and non-infected persons.

It should be noted that there is limited information on the use of surgical masks for the control of a pandemic in settings where there is no identified source of infection. There is no information on respirator use in such scenarios since modern respirators did not exist during the last pandemic. However, respirators are now routinely used to protect employees against occupational hazards, including biological hazards such as tuberculosis, anthrax, and hantavirus. The effectiveness of surgical masks and respirators has been inferred on the basis of the mode of influenza transmission, particle size, and professional judgment.

To offer protection, both surgical masks and respirators must be worn correctly and consistently throughout the time they are being used. If used properly, surgical masks and respirators both have a role in preventing different types of exposures. During an influenza pandemic, surgical masks and respirators should be used in conjunction with interventions that are known to prevent the spread of infection, such as respiratory etiquette, hand hygiene, and avoidance of large gatherings.

Surgical Masks—Surgical masks are used as a physical barrier to protect employees from hazards such as splashes of large droplets of blood or body fluids. Surgical masks also prevent contamination by trapping large particles of body fluids that may contain bacteria or viruses when they are expelled by the wearer, thus protecting other people against infection from the person wearing the surgical mask.

Surgical/procedure masks are used for several different purposes, including the following:

- Placed on sick people to limit the spread of infectious respiratory secretions to others.
- Worn by healthcare providers to prevent accidental contamination of patients' wounds by the organisms normally present in mucus and saliva.

- Worn by employees to protect themselves from splashes or sprays of blood or body fluids; they may also have the effect of keeping contaminated fingers/hands away from the mouth and nose.

Surgical masks are not designed or certified to prevent the inhalation of small airborne contaminants. These small airborne contaminants are too little to see with the naked eye but may still be capable of causing infection. Surgical/procedure masks are not designed to seal tightly against the user's face. During inhalation, much of the potentially contaminated air passes through gaps between the face and the surgical mask, thus avoiding being pulled through the material of the mask and losing any filtration that it may provide. Their ability to filter small particles varies significantly based upon the type of material used to make the surgical mask, and so they cannot be relied upon to protect employees against airborne infectious agents. Only surgical masks that are cleared by the U.S. Food and Drug Administration and legally marketed in the United States have been tested for their ability to resist blood and body fluids.

Respirators—Respirators are designed to reduce an employee's exposure to airborne contaminants. Respirators are designed to fit the face and to provide a tight seal between the respirator's edge and the face. A proper seal between the user's face and the respirator forces inhaled air to be pulled through the respirator's filter material and not through gaps between the face and respirator. Respirators must be used in the context of a comprehensive respiratory protection program, (see OSHA standard 29 CFR 1910.134, or www.osha.gov/SLTC/respiratoryprotection/index.html). It is important to medically evaluate employees to assure that they can perform work tasks while wearing a respirator. Medical evaluation can be as simple as a questionnaire (found in Appendix C of OSHA's Respiratory Protection standard, 29 CFR 1910.134). Employers who have never before needed to consider a respiratory protection plan should note that it can take time to choose a respirator to provide to employees and to arrange for a qualified trainer and provide training, fit testing, and medical evaluation for their employees. If employers wait until an influenza pandemic actually arrives, they may be unable to provide an adequate respiratory protection program in a timely manner.

Types of Respirators

Respirators can be air supplying (e.g., the self-contained breathing apparatus worn by firefighters) or air purifying (e.g., a gas mask that filters hazards from the air). Most employees affected by pandemic influenza who are deemed to need a respirator to minimize the likelihood of exposure to the pandemic influenza virus in the workplace will use some type of air purifying respirator. They are also known as "particulate respirators" because they protect by filtering particles out of the air as you breathe. These respirators protect only against particles not gases or vapors. Since airborne biological agents such as bacteria or viruses are particles, they can be filtered by particulate respirators.

Air purifying respirators can be divided into several types:

- *Disposable or filtering facepiece* respirators, where the entire respirator facepiece is comprised of filter material. This type of respirator is also commonly referred to as an "N95" respirator. It is discarded when it becomes unsuitable for further use due to excessive breathing resistance (e.g., particulate clogging the filter), unacceptable contamination/soiling, or physical damage.
  - *Surgical respirators* are a type of respiratory protection that offers the combined protective properties of both a filtering facepiece respirator and a surgical mask. Surgical N95 respirators are certified by NIOSH as respirators and also cleared by FDA as medical devices which have been designed and tested and shown to be equivalent to surgical masks in certain performance characteristics (resistance to blood penetration, biocompatibility) which are not examined by NIOSH during its certification of N95 respirators.
- *Reusable or elastomeric respirators*, where the facepiece can be cleaned, repaired and reused, but the filter cartridges are discarded and replaced when they become unsuitable for further use. These respirators come in half-mask (covering the mouth and nose) and full-mask (covering mouth, nose, and eyes) types. These respirators can be used with a variety of different cartridges to protect against different hazards. These respirators can also be used with canisters or cartridges that will filter out gases and vapors.
- *Powered air purifying respirators*, (PAPRs) where a battery powered blower pulls contaminated air through filters, then moves the filtered air to the wearer's facepiece. PAPRs are significantly more expensive than other air purifying respirators but they provide higher levels of protection and may also increase the comfort for some users by reducing the physiologic burden associated with negative pressure respirators and providing a constant flow of air on the face. These respirators can also be used with canisters or cartridges that will filter out gases and vapors. It should also be noted that there are hooded PAPRs that do not require employees to be fit tested in order to use them.

All respirators used in the workplace are required to be tested and certified by the National Institute for Occupational Safety and Health (NIOSH). NIOSH-approved respirators are marked with the manufacturer's name, the part number, the protection provided by the filter (e.g., N95), and "NIOSH." This information is printed on the facepiece, exhalation valve cover, or head straps. If a respirator does not have these markings it has not been certified by NIOSH. Those respirators that are surgical N95 respirators are also cleared by the FDA and, therefore, are appropriate for circumstances in which protection from airborne and body fluid contaminants is needed.

When choosing between disposable and reusable respirators, employers should consider their work environment, the nature of pandemics, and the potential for supply chain disruptions. Each pandemic influenza outbreak could last from 6 to 8 weeks and waves of outbreaks may occur over a year or more. While disposable respirators may be more convenient and cheaper on a per unit basis, a reusable respirator may be more economical on a long-term basis and reduce the impact of disruption in supply chains or shortages of respirators.

Classifying Particulate Respirators and Particulate Filters

An N95 respirator is one of nine types of particulate respirators. Respirator filters that remove at least 95 percent of airborne particles during "worst case" testing using the "most-penetrating" size of particle are given a 95 rating. Those that filter out at least 99 percent of the particles under the same conditions receive a 99 rating, and those that filter at least 99.97 percent (essentially 100 percent) receive a 100 rating.

In addition, filters in this family are given a designation of N, R, or P to convey their ability to function in the presence of oils that are found in some work environments.

"N" if they are Not resistant to oil. (e.g., N95, N99, N100)

"R" if they are somewhat Resistant to oil. (e.g., R95, R99, R100)

"P" if they are strongly resistant (i.e., oil Proof). (e.g., P95, P99, P100)

This rating is important in work settings where oils may be present because some industrial oils can degrade the filter performance to the point that it does not filter adequately. Thus, the three filter efficiencies combined with the three oil designations lead to nine types of particulate respirator filter materials. It should be noted that any of the various types of filters listed here would be acceptable for protection against pandemic influenza in workplaces that do not contain oils, particularly if the N95 filter type was unavailable due to shortages.

Replacing Disposable Respirators

Disposable respirators are designed to be used once and are then to be properly disposed of. Once worn in the presence of an infectious patient, the respirator should be considered potentially contaminated with infectious material, and touching the outside of the device should be avoided to prevent self-inoculation (touching the contaminated respirator and then touching one's eyes, nose, or mouth). It should be noted that a once-worn respirator will also be contaminated on its inner surface by the microorganisms present in the exhaled air and oral secretions of the wearer.

If a sufficient supply of respirators is not available during a pandemic, employers and employees may consider reuse as long as the device has not been obviously soiled or damaged (e.g., creased or torn), and it retains its ability to function properly. This practice is not acceptable under normal circumstances and should only be considered under the most dire of conditions. Data on decontamination and/or reuse of respirators for infectious diseases are not available. Reuse may increase the potential for contamination; however, this risk must be balanced against the need to provide respiratory protection. When preparing for a pandemic, employers who anticipate providing respiratory protection to employees for the duration of the pandemic should consider using reusable or elastomeric respirators that are designed to be cleaned, repaired and reused.

Dust or Comfort Masks

Employers and employees should be aware that there are "dust" or "comfort" masks sold at home improvement stores that look very similar to respirators. Some dust masks may even be made by a manufacturer that also produces NIOSH-certified respirators. Unless a mask has been tested and certified by NIOSH, employers do not know if the device will filter very small airborne particles. The occupational use of respirators, including those purchased at home improvement or convenience stores, are still covered by OSHA's Respiratory Protection standard.

Note: Some respirators have an exhalation valve to make it easier for the wearer to breathe. While these respirators provide the same level of particle filtration protection to the wearer, they should not be used by healthcare providers who are concerned about contaminating a sterile field, or provided to known or suspected pandemic patients as a means of limiting the spread of their body fluids to others.

Note: Additional respirator and surgical mask guidance for healthcare workers has been developed and is available at www.pandemicflu.gov/plan/healthcare/maskguidancehc.html. This document, "Interim Guidance on Planning for the Use of Surgical Masks and Respirators in Health Care Settings during an Influenza Pandemic," provides details on the differences between a surgical mask and a respirator, the state of science regarding influenza transmission, and the rationale for determining the appropriate protective device.

STEPS EVERY EMPLOYER CAN TAKE TO REDUCE THE RISK OF EXPOSURE TO PANDEMIC INFLUENZA IN THEIR WORKPLACE

The best strategy to reduce the risk of becoming infected with influenza during a pandemic is to avoid crowded settings and other situations that increase the risk of exposure to someone who may be infected. If it is absolutely necessary to be in a crowded setting, the time spent in a crowd should be as short as possible. Some basic hygiene (see www.cdc.gov/flu/protct/stopgerms.htm) and social distancing precautions that can be implemented in every workplace include the following:

- Encourage sick employees to stay at home.
- Encourage your employees to wash their hands frequently with soap and water or with hand sanitizer if there is no soap or water available. Also, encourage your employees to avoid touching their noses, mouths, and eyes.

- Encourage your employees to cover their coughs and sneezes with a tissue, or to cough and sneeze into their upper sleeves if tissues are not available. All employees should wash their hands or use a hand sanitizer after they cough, sneeze or blow their noses.
- Employees should avoid close contact with their coworkers and customers (maintain a separation of at least 6 feet). They should avoid shaking hands and always wash their hands after contact with others. Even if employees wear gloves, they should wash their hands upon removal of the gloves in case their hand(s) became contaminated during the removal process.
- Provide customers and the public with tissues and trash receptacles, and with a place to wash or disinfect their hands.
- Keep work surfaces, telephones, computer equipment and other frequently touched surfaces and office equipment clean. Be sure that any cleaner used is safe and will not harm your employees or your office equipment. Use only disinfectants registered by the U.S. Environmental Protection Agency (EPA), and follow all directions and safety precautions indicated on the label.
- Discourage your employees from using other employees' phones, desks, offices or other work tools and equipment.
- Minimize situations where groups of people are crowded together, such as in a meeting. Use e-mail, phones and text messages to communicate with each other. When meetings are necessary, avoid close contact by keeping a separation of at least 6 feet, where possible, and assure that there is proper ventilation in the meeting room.
- Reducing or eliminating unnecessary social interactions can be very effective in controlling the spread of infectious diseases. Reconsider all situations that permit or require employees, customers, and visitors (including family members) to enter the workplace. Workplaces which permit family visitors on site should consider restricting/eliminating that option during an influenza pandemic. Work sites with on-site day care should consider in advance whether these facilities will remain open or will be closed, and the impact of such decisions on employees and the business.
- Promote healthy lifestyles, including good nutrition, exercise, and smoking cessation. A person's overall health impacts their body's immune system and can affect their ability to fight off, or recover from, an infectious disease.

WORKPLACES CLASSIFIED AT LOWER EXPOSURE RISK (CAUTION) FOR PANDEMIC INFLUENZA: WHAT TO DO TO PROTECT EMPLOYEES

If your workplace does not require employees to have frequent contact with the general public, basic personal hygiene practices and social distancing can help protect employees at work. Follow the general hygiene and social distancing practices previously recommended for all workplaces (see page 26). Also, try the following:

- Communicate to employees what options may be available to them for working from home.
- Communicate the office leave policies, policies for getting paid, transportation issues, and day care concerns.
- Make sure that your employees know where supplies for hand hygiene are located.
- Monitor public health communications about pandemic flu recommendations and ensure that your employees also have access to that information.
- Work with your employees to designate a person(s), website, bulletin board or other means of communicating important pandemic flu information.

More information about protecting employees and their families can be found at: www.pandemicflu.gov.

WORKPLACES CLASSIFIED AT MEDIUM EXPOSURE RISK FOR PANDEMIC INFLUENZA: WHAT TO DO TO PROTECT EMPLOYEES

Medium risk workplaces require frequent close contact between employees or with the general public (such as high-volume retail stores). If this contact cannot be avoided, there are practices to reduce the risk of infection. In addition to the basic work practices that every workplace should adopt (see page 26), medium risk occupations require employers to address enhanced safety and health precautions. Below are some of the issues that employers should address when developing plans for workplace safety and health during a pandemic.

Work Practice and Engineering Controls

- Instruct employees to avoid close contact (within 6 feet) with other employees and the general public. This can be accomplished by simply increasing the distance between the employee and the general public in order to avoid contact with large droplets from people talking, coughing or sneezing.
- Some organizations can expand internet, phone-based, drive-through window, or home delivery customer service strategies to minimize face-to-face contact. Work with your employees to identify new ways to do business that can also help to keep employees and customers safe and healthy.

- Communicate the availability of medical screening or other employee health resources (e.g., on-site nurse or employee wellness program to check for flu-like symptoms before employees enter the workplace).
- Employers also should consider installing physical barriers, such as clear plastic sneeze guards, to protect employees where possible (such as cashier stations).

Administrative Controls

- Work with your employees so that they understand the office leave policies, policies for getting paid, transportation issues, and day care concerns.
- Make sure that employees know where supplies for hand and surface hygiene are located.
- Work with your employees to designate a person(s), website, bulletin board or other means of communicating important pandemic flu information.
- Use signs to keep customers informed about symptoms of the flu, and ask sick customers to minimize contact with your employees until they are well.
- Your workplace may consider limiting access to customers and the general public, or ensuring that they can only enter certain areas of your workplace.

Personal Protective Equipment (PPE)

Employees who have high-frequency, close contact with the general population that cannot be eliminated using administrative or engineering controls, and where contact with symptomatic ill persons is not expected should use personal protective equipment to prevent sprays of potentially infected liquid droplets (from talking, coughing, or sneezing) from contacting their nose or mouth. A surgical mask will provide such barrier protection. Use of a respirator may be considered if there is an expectation of close contact with persons who have symptomatic influenza infection or if employers choose to provide protection against a risk of airborne transmission. It should be noted that wearing a respirator may be physically burdensome to employees, particularly when the use of PPE is not common practice for the work task. In the event of a shortage of surgical masks, a reusable face shield that can be decontaminated may be an acceptable method of protecting against droplet transmission of an infectious disease but will not protect against airborne transmission, to the extent that disease may spread in that manner.

Eye protection generally is not recommended to prevent influenza infection although there are limited examples where strains of influenza have caused eye infection (conjunctivitis). At the time of a pandemic, health officials will assess whether risk of conjunctival infection or transmission exists for the specific pandemic viral strain.

Employees should wash hands frequently with soap or sanitizing solutions to prevent hands from transferring potentially infectious material from surfaces to their mouths or noses. While employers and employees may choose to wear gloves, the exposure of concern is touching the mouth and nose with a contaminated hand and not exposure to the virus through non-intact skin (for example, cuts or scrapes). While the use of gloves may make employees more aware of potential hand contamination, there is no difference between intentional or unintentional touching of the mouth, nose or eyes with either a contaminated glove or a contaminated hand. If an employee does wear gloves, they should always wash their hands with soap or sanitizing solution immediately after removal to ensure that they did not contaminate their hand(s) while removing them.

When selecting PPE, employers should consider factors such as function, fit, ability to be decontaminated, disposal, and cost. Sometimes, when a piece of PPE will have to be used repeatedly for a long period of time, a more expensive and durable piece of PPE may be less expensive in the long run than a disposable piece of PPE. For example, in the event of a pandemic, there may be shortages of surgical masks. A reusable face shield that can be decontaminated may become the preferred method of protecting against droplet transmission in some workplaces. It should be noted that barrier protection, such as a surgical mask or face shield, will protect against droplet transmission of an infectious disease but will not protect against airborne transmission, to the extent that the disease may be spread in that manner. Each employer should select the combination of PPE that protects employees in their particular workplace. It should also be noted that wearing PPE may be physically burdensome to employees, particularly when the use of PPE is not common practice for the work task.

Educate and train employees about the protective clothing and equipment appropriate to their current duties and the duties which they may be asked to assume when others are absent. Employees may need to be fit tested and trained in the proper use and care of a respirator. Also, it is important to train employees to put on (don) and take off (doff) PPE in the proper order to avoid inadvertent self-contamination (www.osha.gov/SLTC/respiratoryprotection/index.html). During a pandemic, recommendations for PPE use in particular occupations may change, depending on geographic proximity to active cases, updated risk assessments for particular employees, and information on PPE effectiveness in preventing the spread of influenza.

WORKPLACES CLASSIFIED AT VERY HIGH OR HIGH EXPOSURE RISK FOR PANDEMIC INFLUENZA: WHAT TO DO TO PROTECT EMPLOYEES

If your workplace requires your employees to have contact with people that are known or suspected to be infected with the pandemic virus, there are many practices that can be used to reduce the risk of infection and to protect your employees. Additional guidance for very high and high exposure risk workplaces, such as health care facilities, can be found at: www.pandemicflu.gov and www.osha.gov.

Very high and high exposure risk occupations require employers to address enhanced safety and health precautions in addition to the basic work practices that every workplace should adopt (see page 26). Employers should also be aware that working in a high risk occupation can be stressful to both employees and their families. Employees in high risk occupations may have heightened concern about their own safety and possible implications for their family. Such workplaces may experience greater employee absenteeism than other lower risk workplaces. Talk to your employees about resources that can help them in the event of a pandemic crisis. Keeping the workplace safe is everyone's priority. More information about protecting employees and their families can be found at: www.pandemicflu.gov.

Work Practice and Engineering Controls

Employers should ensure that employees have adequate training and supplies to practice proper hygiene. Emergency responders and other essential personnel who may be exposed while working away from fixed facilities should be provided with hand sanitizers that do not require water so that they can decontaminate themselves in the field. Employers should work with employees to identify ways to modify work practices to promote social distancing and prevent close contact (within 6 feet), where possible. Employers should also consider offering enhanced medical monitoring of employees in very high and high risk work environments.

In certain limited circumstances ventilation is recommended for high and very high risk work environments. While proper ventilation can reduce the risk of transmission for healthcare workers in the same room as infectious patients, it cannot be relied upon as the sole protective measure. Thus, a combination of engineering controls and personal protective equipment will be needed.

- When possible, health care facilities equipped with isolation rooms should use them when performing aerosol generating procedures for patients with known or suspected pandemic influenza.
- Laboratory facilities that handle specimens for known or suspected pandemic patients will also require special precautions associated with a Bio-Safety Level 3 facility. Some recommendations can be found at: www.cdc.gov/flu/h2n2bs13.htm.

Employers should also consider installing physical barriers, such as clear plastic sneeze guards, to protect employees where possible (for example, reception or intake areas). The use of barrier protections, such as sneeze guards, is common practice for both infection control and industrial hygiene.

Administrative Controls (Isolation Precautions)

If working in a health care facility, follow existing guidelines and facility standards of practice for identifying and isolating infected individuals and for protecting employees. See the U.S. Department of Health and Human Services' pandemic influenza plan for health care facilities at: www.hhs.gov/pandemicflu/plan/sup4.html.

Personal Protective Equipment (PPE)

Those who work closely with (either in contact with or within 6 feet) people known or suspected to be infected with pandemic influenza should wear:

- Respiratory protection for protection against small droplets from talking, coughing or sneezing and also from small airborne particles of infectious material.
  - N95 or higher rated filter for most situations.
  - Supplied air respirator (SAR) or powered air purifying respirator (PAPR) for certain high risk medical or dental procedures likely to generate bioaerosols.
  - Use a surgical respirator when both respiratory protection and resistance to blood and body fluids is necessary.
- Face shields may also be worn on top of a respirator to prevent bulk contamination of the respirator. Certain respirator designs with forward protrusions (duckbill style) may be difficult to properly wear under a face shield. Ensure that the face shield does not prevent airflow through the respirator.
- Medical/surgical gowns or other disposable/decontaminable protective clothing.
- Gloves to reduce transfer of infectious material from one patient to another.
- Eye protection if splashes are anticipated.

The appropriate form of respirator will depend on the type of exposure and on the transmission pattern of the particular strain of influenza. See the National Institute for Occupational Safety and Health (NIOSH) Respirator Selection Logic at: www.cdc.gov/niosh/docs/2005-100.

Educate and train employees about the protective clothing and equipment appropriate to their current duties and the duties which they may be asked to assume when others are absent. Education and training material should be easy to understand and available in the appropriate language and literacy level for all employees. Employees need to be fit tested and trained in the proper use and care of a respirator. It is also important to train employees to put on (don) and take off (doff) PPE in the proper order to avoid inadvertent self-contamination (www.osha.gov/SLTC/respiratoryprotection/index.html). Employees who dispose of PPE and other infectious waste must also be trained and provided with appropriate PPE.

During a pandemic, recommendations for PPE use in particular occupations may change depending on geographic location, updated risk assessments for particular employees, and information on PPE effectiveness in preventing the spread of influenza. Additional respirator and surgical mask guidance for healthcare workers has been developed and is available at www.pandemicflu.gov/plan/healthcare/maskguidancehc.html. This document, Interim Guidance on Planning for the Use of Surgical Masks and Respirators in Health Care Settings during an Influenza Pandemic, provides details on the differences between a surgical mask and a respirator, the state of science regarding influenza transmission, and the rationale for determining the appropriate protective device.

WHAT EMPLOYEES LIVING ABROAD OR WHO TRAVEL INTERNATIONALLY FOR WORK SHOULD KNOW

Employees living abroad and international business travelers should note that other geographic areas have different influenza seasons and will likely be affected by a pandemic at different times than the United States. The U.S. Department of State emphasizes that, in the event of a pandemic, its ability to assist Americans traveling and residing abroad may be severely limited by restrictions on local and international movement imposed for public health reasons, either by foreign governments and/or the United States. Furthermore, American citizens should take note that the Department of State cannot provide Americans traveling or living abroad with medications or supplies even in the event of a pandemic.

In addition, the Department of State has asked its embassies and consulates to consider preparedness measures that take into consideration the fact that travel into or out of a country may not be possible, safe, or medically advisable during a pandemic. Guidance on how private citizens can prepare to shelter in place, including stocking food, water, and medical supplies, is available at the www.pandemicflu.gov website. Embassy stocks cannot be made available to private American citizens abroad, therefore, employers and employees are encouraged to prepare appropriately. It is also likely that governments will respond to a pandemic by imposing public health measures that restrict domestic and international movement, further limiting the U.S. government's ability to assist Americans in these countries. As it is possible that these measures may be implemented very quickly, it is important that employers and employees plan appropriately.

More information on pandemic influenza planning for employees living and traveling abroad can be found at: www.pandemicflu.gov/travel/index.html; www.cdc.gov/travel; www.state.gov/travelandbusiness

FOR MORE INFORMATION

Federal, state and local government agencies are your best source of information should an influenza pandemic take place. It is important to stay informed about the latest developments and recommendations since specific guidance may change based upon the characteristics of the eventual pandemic influenza strain, (for example, severity of disease, importance of various modes of transmission).

Below are several recommended websites that you can rely on for the most current and accurate information:

www.pandemicflu.gov
(Managed by the Department of Health and Human Services; offers one-stop access, including toll-free phone numbers, to U.S. government avian and pandemic flu information.)

www.osha.gov
(Occupational Safety and Health Administration website)

www.cdc.gov/niosh
(National Institute for Occupational Safety and Health website)

www.cdc.gov
(Centers for Disease Control and Prevention website)

www.fda.gov/cdrh/ppe/fluoutbreaks.html
(U.S. Food and Drug Administration website)

OSHA ASSISTANCE

OSHA can provide extensive help through a variety of programs, including technical assistance about effective safety and health programs, state plans, workplace consultations, voluntary protection programs, strategic partnerships, training and education, and more. An overall commitment to workplace safety and health can add value to your business, to your workplace and to your life.

Safety and Health Program Management Guidelines

Effective management of employee safety and health protection is a decisive factor in reducing the extent and severity of work-related injuries and illnesses and their related costs. In fact, an effective safety and health program forms the basis of good employee protection and can save time and money (about $4 for every dollar spent) and increase productivity and reduce employee injuries, illnesses and related workers' compensation costs.

To assist employers and employees in developing effective safety and health programs, OSHA published recommended *Safety and Health Program Management Guidelines* (*54 Federal Register* (16): 3904–3916, January 26, 1989). These voluntary guidelines apply to all places of employment covered by OSHA.

The guidelines identify four general elements critical to the development of a successful safety and health management program:

- Management leadership and employee involvement.
- Work analysis.
- Hazard prevention and control.
- Safety and health training.

The guidelines recommend specific actions, under each of these general elements, to achieve an effective safety and health program. The *Federal Register* notice is available online at www.osha.gov.

State Programs

The Occupational Safety and Health Act of 1970 (OSH Act) encourages states to develop and operate their own job safety and health plans. OSHA approves and monitors these plans. Twenty-four states, Puerto Rico and the Virgin Islands currently operate approved state plans: 22 cover both private and public (state and local government) employment; Connecticut, New Jersey, New York and the Virgin Islands cover the public sector only. States and territories with their own OSHA-approved occupational safety and health plans must adopt standards identical to, or at least as effective as, the Federal standards.

Consultation Services

Consultation assistance is available on request to employers who want help in establishing and maintaining a safe and healthful workplace. Largely funded by OSHA, the service is provided at no cost to the employer. Primarily developed for smaller employers with more hazardous operations, the consultation service is delivered by state governments employing professional safety and health consultants. Comprehensive assistance includes an appraisal of all mechanical systems, work practices and occupational safety and health hazards of the workplace and all aspects of the employer's present job safety and health program. In addition, the service offers assistance to employers in developing and implementing an effective safety and health program. No penalties are proposed or citations issued for hazards identified by the consultant. OSHA provides consultation assistance to the employer with the assurance that his or her name and firm and any information about the workplace will not be routinely reported to OSHA enforcement staff.

Under the consultation program, certain exemplary employers may request participation in OSHA's Safety and Health Achievement Recognition Program (SHARP). Eligibility for participation in SHARP includes receiving a comprehensive consultation visit, demonstrating exemplary achievements in workplace safety and health by abating all identified hazards and developing an excellent safety and health program.

Employers accepted into SHARP may receive an exemption from programmed inspections (not complaint or accident investigation inspections) for a period of one year. For more information concerning consultation assistance, see the OSHA website at www.osha.gov.

Voluntary Protection Program (VPP)

Voluntary Protection Programs and on-site consultation services, when coupled with an effective enforcement program, expand employee protection to help meet the goals of the OSH Act. The three levels of VPP are Star, Merit, and Star Demonstration designed to recognize outstanding achievements by companies that have successfully incorporated comprehensive safety and health programs into their total management system. The VPPs motivate others to achieve excellent safety and health results in the same outstanding way as they establish a cooperative relationship between employers, employees and OSHA.

For additional information on VPP and how to apply, contact the OSHA regional offices listed at the end of this publication.

Strategic Partnership Program

OSHA's Strategic Partnership Program, the newest member of OSHA's cooperative programs, helps encourage, assist and recognize the efforts of partners to eliminate serious workplace hazards and achieve a high level of employee safety and health. Whereas OSHA's Consultation Program and VPP entail one-on-one relationships between OSHA and individual worksites, most strategic partnerships seek to have a broader impact by building cooperative relationships with groups of employers and employees. These partnerships are voluntary, cooperative relationships between OSHA, employers, employee representatives and others (e.g., trade unions, trade and professional associations, universities and other government agencies).

For more information on this and other cooperative programs, contact your nearest OSHA office, or visit OSHA's website at www.osha.gov.

Alliance Programs

The Alliance Program enables organizations committed to workplace safety and health to collaborate with OSHA to prevent injuries and illnesses in the workplace. OSHA and the Alliance participants work together to reach out to, educate and lead the nation's employers and their employees in improving and advancing workplace safety and health.

Groups that can form an Alliance with OSHA include employers, labor unions, trade or professional groups, educational institutions and government agencies. In some cases, organizations may be building on existing relationships with OSHA that were developed through other cooperative programs.

There are few formal program requirements for Alliances and the agreements do not include an enforcement component. However, OSHA and the participating organizations must define, implement and meet a set of short-and long-term goals that fall into three categories: training and education; outreach and communication; and promoting the national dialogue on workplace safety and health.

OSHA Training and Education

OSHA area offices offer a variety of information services, such as compliance assistance, technical advice, publications, audiovisual aids and speakers for special engagements. OSHA's Training Institute in Arlington Heights, IL, provides basic and advanced courses in safety and health for Federal and state compliance officers, state consultants, Federal agency personnel, and private sector employers, employees and their representatives.

The OSHA Training Institute also has established OSHA Training Institute Education Centers to address the increased demand for its courses from the private sector and from other Federal agencies. These centers are nonprofit colleges, universities and other organizations that have been selected after a competition for participation in the program.

OSHA also provides funds to nonprofit organizations, through grants, to conduct workplace training and education in subjects where OSHA believes there is a lack of workplace training. Grants are awarded annually. Grant recipients are expected to contribute 20 percent of the total grant cost.

For more information on grants, training and education, contact the OSHA Training Institute, Office of Training and Education, 2020 South Arlington Heights Road, Arlington Heights, IL 60005, (847) 297-4810 or see "Outreach" on OSHA's website at www.osha.gov. For further information on any OSHA program, contact your nearest OSHA area or regional office listed at the end of this publication.

Information Available Electronically

OSHA has a variety of materials and tools available on its website at www.osha.gov. These include *eTools* such as *Expert Advisors, Electronic Compliance Assistance Tools (e-cats), Technical Links;* regulations, directives and publications; videos and other information for employers and employees. OSHA's software programs and compliance assistance tools walk you through challenging safety and health issues and common problems to find the best solutions for your workplace.

A wide variety of OSHA materials, including standards, interpretations, directives, and more, can be purchased on CD-ROM from the U.S. Government Printing Office, Superintendent of Documents, phone toll-free (866) 512-1800.

OSHA Publications

OSHA has an extensive publications program. For a listing of free or sales items, visit OSHA's website at www.osha.gov or contact the OSHA Publications Office, U.S. Department of Labor, 200 Constitution Avenue, NW, N-3101, Washington, DC 20210. Telephone (202) 693-1888 or fax to (202) 693-2498.

Contacting OSHA

To report an emergency, file a complaint, or seek OSHA advice, assistance, or products, call (800) 321-OSHA or contact your nearest OSHA Regional or Area office listed at the end of this publication. The teletypewriter (TTY) number is (877) 889-5627.

Written correspondence can be mailed to the nearest OSHA Regional or Area Office listed at the end of this publication or to OSHA's national office at: U.S. Department of Labor, Occupational Safety and Health Administration, 200 Constitution Avenue, N.W., Washington, DC 20210.

By visiting OSHA's website at www.osha.gov, you can also:

- file a complaint online,
- submit general inquiries about workplace safety and health electronically, and
- find more information about OSHA and occupational safety and health.

OSHA REGIONAL OFFICES

Region I
(CT,* ME, MA, NH, RI, VT*)
JFK Federal Building, Room E340
Boston, MA 02203
(617) 565-9860

Region II
(NJ,* NY,* PR,* VI*)
201 Varick Street, Room 670
New York, NY 10014
(212) 337-2378

Region III
(DE, DC, MD,* PA, VA,* WV)
The Curtis Center
170 S. Independence Mall West
Suite 740 West
Philadelphia, PA 19106-3309
(215) 861-4900

Region IV
(AL, FL, GA, KY,* MS, NC,* SC,* TN*)
61 Forsyth Street, SW
Atlanta, GA 30303
(404) 562-2300

Region V
(IL, IN,* MI,* MN,* OH, WI)
230 South Dearborn Street
Room 3244
Chicago, IL 60604
(312) 353-2220

Region VI
(AR, LA, NM,* OK, TX)
525 Griffin Street, Room 602
Dallas, TX 75202
(214) 767-4731 or 4736 x 224

Region VII
(IA,* KS, MO, NE)
City Center Square
1100 Main Street, Suite 800
Kansas City, MO 64105
(816) 426-5861

Region VIII
(CO, MT, ND, SD, UT,* WY*)
1999 Broadway, Suite 1690
PO Box 46550
Denver, CO 80202-5716
(720) 264-6550

Region IX
(American Samoa, AZ,* CA,* HI,* NV,*
Northern Mariana Islands)
71 Stevenson Street, Room 420
San Francisco, CA 94105
(415) 975-4310

Region X
(AK,* ID, OR,* WA*)
1111 Third Avenue, Suite 715
Seattle, WA 98101-3212
(206) 553-5930

* These states and territories operate their own OSHA-approved job safety and health programs (Connecticut, New Jersey, New York and the Virgin Islands plans cover public employees only). States with approved programs must adopt standards identical to, or at least as effective as, the Federal standards.

Note: To get contact information for OSHA Area Offices, OSHA-approved State Plans and OSHA Consultation Projects, please visit us online at www.osha.gov or call us at 1-800-321-OSHA.

INDUSTRY SELF-ASSESSMENT CHECKLIST FOR FOOD SECURITY

U.S. Department of Agriculture
Food Safety and Inspection Service

It is vital that all food slaughter and processing establishments, and all import, export, and identification warehouses take steps to ensure the security of their operations. USDA's Food Safety and Inspection Service (FSIS) created this self-assessment instrument to provide a tool for establishments to assess the extent to which they have secured their operations. The contents of the instrument are based primarily on the food security guidelines that FSIS published in 2002, *Food Security Guidelines for Food Processors*, available at www.fsis.usda.gov. Those guidelines identify security measures that establishments can adopt to enhance the security of their operations.

The checklist consists of the following (9) sections:

I. Food Security Plan Management
II. Outside Security
III. Inside Security
IV. Slaughter and Processing Security
V. Storage Security
VI. Shipping and Receiving Security
VII. Water and Ice Supply Security
VIII. Mail Handling Security
IX. Personnel Security

To use the checklist, read each question under each section and check the response that best describes the food security practice in the establishment. If a question is not applicable, check "N/A." For example, if an establishment only conducts processing activities, then questions that ask about live animals or slaughter operations would not apply. Similarly, if an establishment only conducts import/export inspection activities, then questions related to processing or slaughter would not apply. A "Yes" response for every question is desirable but not expected due to the layering of certain security measures. A "No" answer on a question does not necessarily constitute a breach in security. The establishment might have other management strategies or activities conducted at different frequencies that accomplish food security goals.

A "No" should, however, trigger a critical thought process in establishment operators on whether management decisions should be made regarding additional security measures they may need to put in place at the particular operational sector/area of the establishment covered by the "No" response. In addition, Appendix 1 lists resources and websites that discuss additional security measures for establishments. Resources/websites specific to a section or question are shown at the corresponding section/question throughout the checklist for quick and easy reference. "NA" responses should be reviewed periodically to validate them against current operations.

The final outcome of this self-assessment should provide establishments with a relative measure of overall security of their operations and guide them in the development and/or revision of their food security strategies.

This checklist is one of several outreach efforts by FSIS to assist the industry to enhance the security of its regulated food products. Model food security plans have also been developed for voluntary use by the industry. The Agency is also considering additional measures that may be appropriate to ensure the safety and security of meat, poultry and egg products under certain elevated threat conditions specific to food and agriculture.

I. FOOD SECURITY PLAN MANAGEMENT

A food security plan is a written document developed using established risk management procedures and consists of specific standard operating procedures for preventing intentional product tampering and responding to threats or actual incidents of intentional product tampering.

1. Does this establishment have a written food security plan?
   □ Yes
   □ No [GO TO QUESTION 3]

2. Which of the following procedures, plans, or information are either included in the food security plan or have been put in place as a result of the food security plan? *(Check "Yes" or "No" for each item.)*

	Yes	No
Is there a designated person or team to implement and oversee the food security plan?	□	□
Are members of the food security management team trained in all provisions of the food security plan?	□	□
Are periodic drills conducted on operational elements of the food security plan?	□	□
Are regular food security inspections conducted to verify key provisions of the food security plan?	□	□
Is the security plan reviewed (and revised if necessary) periodically?	□	□
Are the details of food security procedures kept confidential?	□	□
Is the emergency contact information for local, state, and federal government homeland security authorities and public health officials included in the security plan?	□	□
State contact list: www.whitehouse.gov/homeland/contactmap.html		
Is the above contact information periodically reviewed and updated?	□	□
Is there an established liaison between plant officials and the local homeland security officials and other law enforcement officials?	□	□
Is there an established relationship between the establishment and the appropriate analytical laboratories for possible assistance in investigation of product tampering cases?	□	□
Are procedures for responding to threats of product tampering included in the plan?	□	□
Are procedures for responding to actual incidents of product tampering detailed in the plan? http://www.state.tn.us/agriculture/security/fsig.html	□	□
Are communication procedures for notifying law enforcement, public health officials, and FSIS inspectors in-charge when a food security threat is received or when evidence of actual product tampering is observed included in the plan?	□	□
Are procedures in the plan for corrective action in cases of product tampering to ensure that adulterated or potentially injurious products do not enter commerce?	□	□
Are procedures in the plan for safe handling and disposal of contaminated products?	□	□
Are employees encouraged to report signs of possible product tampering or breaks in food security system (e.g., award system)?	□	□
Are evacuation procedures in the security plan? Visit www.osha.gov/dep/evacmatrix/index.html for guidance material provided by the U.S. Department of Labor, Occupational Safety and Health Administration	□	□
Are procedures in place to restrict access to the facility during an emergency to authorized personnel only?	□	□
Are designated entry points for emergency personnel clearly marked?	□	□
Does the establishment have a documented recall plan?	□	□
Are procedures in the recall plan reviewed and updated as necessary?	□	□
Do recall procedures ensure segregation and disposition of recalled products?	□	□

II. OUTSIDE SECURITY

3. Which of the following security procedures does this establishment have in place for the exterior of this establishment? *(Check "Yes" or "No" for each procedure.)*

	Yes	No
Are the plant's boundaries and grounds secured to prevent entry by unauthorized persons (e.g., by locked fence or gate)?	□	□
Are "No Trespassing" signs posted at plant's boundaries?	□	□
Is there sufficient outside lighting to allow detection of unusual activities on any part of the establishment outside premises during non-daylight hours?	□	□
Do emergency exits have self-locking doors and/or alarms?	□	□
Is positive identification required to control entry of visitors to the plant (e.g., picture IDs or sign-in/sign-out at entrance)?	□	□
Is an updated list of establishment personnel with open or restricted access to the establishment maintained at the security office or another secure location?	□	□

4. Are the following secured with locks, seals, or sensors at all times to prevent entry by unauthorized persons? *(Check "Yes" or "No" for each item, or "N/A" if the item is not applicable.)*

	Yes	No	N/A
Outside doors and gates?	□	□	□
Windows?	□	□	□
Roof openings?	□	□	□
Vent openings?	□	□	□
Trailer (truck) bodies?	□	□	□
Tanker truck hatches?	□	□	□
Railcars?	□	□	□
Bulk storage tanks?	□	□	□

5. Which of the following security procedures does this establishment have in place for vehicles entering the establishment? *(Check "Yes" or "No" for each procedure.)*

	Yes	No
Are *incoming* private vehicles (e.g., employees or visitors) inspected for unusual cargo or activity?	□	□
Are *outgoing* private vehicles (e.g., employees or visitors) inspected for unusual cargo or activity?	□	□
Are *incoming* commercial vehicles (e.g., delivery trucks) inspected for unusual cargo or activity?	□	□
Are *outgoing* commercial vehicles (e.g., delivery trucks) inspected for unusual cargo or activity?	□	□

Are *incoming* tanker truck shipments checked for documentation of chain of custody prior to loading?	□	□
Are *employee* vehicles identified using placards, decals, or some other form of visual identification?	□	□
Are authorized *visitor/quest* vehicles identified using placards, decals, or some other form of visual identification?	□	□

III. GENERAL INSIDE SECURITY

6. Which of the following security procedures does this establishment have in place within the interior of this establishment? *(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable.)*

	Yes	No	N/A
Is emergency lighting provided in the establishment?	□	□	□
Is active surveillance of the inside facility and operations maintained?	□	□	□
Are emergency alert systems tested periodically?	□	□	□
Are the locations of controls for emergency alert systems clearly marked?	□	□	□
Are all restricted areas (i.e., areas where only authorized employees have access) within the plant clearly marked?	□	□	□
Are visitors, guests, and other non-establishment employees (e.g., contractors, salespeople, truck drivers) restricted to non-product areas unless accompanied by an authorized establishment employee?	□	□	□
Are updated plant layout schematics provided at strategic and secured locations?	□	□	□
Are procedures in place to check toilets, maintenance closets, personal lockers, and storage areas for suspicious packages?	□	□	□
Is an inventory of tools and utensils (e.g., knives) conducted regularly as needed to ensure security?	□	□	□
Is an inventory of keys to secured areas of the facility conducted regularly to ensure security?	□	□	□
Are ventilation systems constructed in a manner that provides for isolation of contaminated areas or rooms?	□	□	□

7. Are the central controls for the following restricted (e.g., by locked door/gate or limiting access to designated employees) to prevent access by unauthorized persons?
Check "Yes" or "No" for each item, or "N/A" if the item is not applicable.
www.cdc.gov/niosh/bldvent/2002-139.html

	Yes	No	N/A
Heating, Ventilation, and Air Conditioning systems?	□	□	□
Propane Gas?	□	□	□
Water systems?	□	□	□

Electricity?	□	□	□
Disinfection systems?	□	□	□
Clean-in-place (CIP) systems?	□	□	□

8. Does this establishment collect and analyze samples in-house?
   □ Yes
   □ No [GO TO QUESTION 10]

9. Which of the following security procedures does this establishment have in place for its in-plant laboratory facilities, equipment, and operations? *(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable [e.g., this establishment does not use live cultures of pathogenic bacteria].)*

	Yes	No	N/A
Is access to the in-plant laboratory facilities restricted to authorized employees? (e.g., by locked door, pass card, etc.)	□	□	□
Is a procedure in place to control receipt of samples received from other establishments?	□	□	□
Is a procedure in place to receive and securely store reagents?	□	□	□
Is a procedure in place to control and dispose of reagents?	□	□	□
Is a procedure in place to receive and securely store live cultures of pathogenic bacteria?	□	□	□
Is a procedure in place to dispose of live cultures of pathogenic bacteria?	□	□	□

10. Does this establishment use a computer system to monitor processing operations?
    □ Yes
    □ No [GO TO QUESTION 12]

11. Which of the following security procedures does this establishment have in place for its computer systems? *(Check "Yes" or "No" for each procedure.)* http://www.fiu.edu/security.guidelines.html

	Yes	No
Is the access to the system password-protected? http://www.umich.edu/~policies/pw-security.html	□	□
Are firewalls built into the computer network?	□	□
Is the system using a current virus detection system?	□	□

IV. SLAUGHTER AND PROCESSING SECURITY

12. Which of the following security procedures does this establishment have in place for its slaughter and processing operations? *(Check "Yes" or "No" for*

each procedure, or "N/A" if the procedure is not applicable [e.g., this establishment does not mix or batch ingredients].)

	Yes	No	N/A*
Is access to product production/slaughter and holding pen areas restricted to establishment employees and FSIS inspection personnel only?	□	□	□
Is the mixing and batching of product and ingredients and other operations where large amounts of exposed product are handled continuously monitored?	□	□	□
Are lines that handle and transfer products, water, oil, or other ingredients monitored to ensure integrity?	□	□	□
Is the packaging integrity of ingredients examined for evidence of tampering before use?	□	□	□
Is the restricted access to in-plant irradiation equipment and materials clearly marked and maintained?	□	□	□
Are records maintained to ensure the capability to trace-back raw materials to suppliers?	□	□	□
Are records maintained to ensure the capability to trace-forward finished products to vendors?	□	□	□

*"N/A" RESPONSE POSSIBLE IN ABOVE SECTION FOR IMPORT, EXPORT, AND ID ESTABLISHMENTS.

V. STORAGE SECURITY

13. Which of the following security procedures does this establishment have in place for its storage areas? *(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable [e.g., this establishment does not use restricted ingredients].)*

	Yes	No	N/A
Is access to raw product storage areas, including holding coolers restricted (e.g., by locked door/gate) to designated employees?	□	□	□
Is an access log maintained for raw product storage areas?	□	□	□
Is access to non-meat ingredient storage areas restricted to designated employees only?	□	□	□
Is an access log maintained for ingredient storage areas?	□	□	□
Is access to finished product storage areas restricted to designated employees?	□	□	□
Is access to external storage facilities restricted to designated employees only?	□	□	□
Are silo storage tanks for raw egg product and other bulk ingredients (syrup, oils, etc.) maintained under lock and seal?	□	□	□
Are silo storage tanks for pasteurized egg product and other bulk finished products maintained under lock and seal?	□	□	□
Are silo storage tanks for inedible egg product and other bulk inedible products maintained under lock and seal?	□	□	□

	Yes	No	N/A
Are periodic security inspections of storage facilities (including temporary storage vehicles) conducted?	□	□	□
Are records maintained on facility security inspections results?	□	□	□
Is the inventory of restricted ingredients (i.e., nitrites, etc) reconciled against the actual use of such ingredients on a regular basis?	□	□	□
Are product labels and packaging held in a secure area to prevent theft and misuse?	□	□	□
Is the inventory of finished products regularly checked for unexplained additions and withdrawals from existing stock?	□	□	□

14. Which of the following security procedures does this establishment have in place for the storage of hazardous materials/chemicals such as pesticides, industrial chemicals, cleaning materials, sanitizers, and disinfectants? *(Check "Yes" or "No" for each procedure.)*

	Yes	No
Is the access to inside and outside storage areas for hazardous materials/chemicals such as pesticides, industrial chemicals, cleaning materials, sanitizers, and disinfectants restricted to designated employees?	□	□
Are hazardous material/chemical storage areas separated from production areas of plant?	□	□
Is a regular inventory of hazardous materials/chemicals maintained?	□	□
Are discrepancies in daily inventory of hazardous materials/chemicals immediately investigated?	□	□
Are the storage areas for hazardous materials/chemicals constructed and safely vented in accordance with national or local building codes?	□	□
Is a procedure in place to receive and securely store hazardous chemicals?	□	□
Is a procedure in place to control disposition of hazardous chemicals?	□	□

VI. SHIPPING AND RECEIVING SECURITY

Visit: http://www.fsis.usda.gov/oa/topics/transportguide.htm

15. Which of the following security procedures does this establishment have in place for its shipping and receiving operations? *(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable [e.g., no tanker trucks on premises].)*

	Yes	No	N/A
Are trailers on the premises maintained under lock and/or seal when not being loaded or unloaded?	□	□	□
Are tanker trucks on the premises maintained under lock and seal when not being loaded or unloaded?	□	□	□
Is the loading and unloading of vehicles transporting raw materials, finished products, or other materials used in food processing closely monitored?	□	□	□

16. Which of the following security procedures does this establishment have in place for handling outgoing shipments? *(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable [e.g., no tanker trucks on premises].)*

	Yes	No	N/A
Are outgoing shipments sealed with tamper-evident seals?	□	□	□
Are the seal numbers on outgoing shipment documented on the shipping documents?	□	□	□
Are tanker trucks visually inspected to detect the presence of any material, solid or liquid, in tanks prior to loading liquid products?	□	□	□
Are records maintained of the above inspections of tanker trucks?	□	□	□
Are chain-of-custody records maintained for tanker trucks?	□	□	□

17. Which of the following security procedures does this establishment have in place for handling incoming shipments? *(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable [e.g., this establishment does not receive live animals].)*

	Yes	No	N/A
Is access to loading docks controlled to avoid unverified or unauthorized deliveries?	□	□	□
Is advance notification from suppliers (by phone, e-mail, or fax) required for all incoming deliveries?	□	□	□
Are suspicious alterations in the shipping documents immediately investigated?	□	□	□
Are all deliveries verified against the roster of scheduled deliveries?	□	□	□
Are unscheduled deliveries held outside facility premises pending verification?	□	□	□
Are off-hour deliveries accepted?	□	□	□
If off-hour deliveries are accepted, is prior notice of the delivery required?	□	□	□
If off-hour deliveries are accepted, is the presence of authorized individual to verify and receive the delivery required?	□	□	□
Is the integrity of internal compartments in the truck, lot packaging, or in-transit security checks for less-than-truckload (LTL) or partial load shipments of materials verified?	□	□	□
Are incoming shipments of raw product, ingredients, and finished products required to be sealed with tamper-evident or numbered seals (and documented in the shipping documents) which are verified prior to entry?	□	□	□
Is the integrity of incoming shipments of raw product, ingredients, and finished products checked at receiving dock for evidence of tampering?	□	□	□
Is the FSIS Public Health Veterinarian notified immediately when animals with unusual behavior and/or symptoms are received? http://www.inspection.gc.ca/english/ops/secur/livbete.shtml	□	□	□

	Yes	No	N/A
Are the feed and drinking water supplies for live animals protected from possible intentional contamination?	□	□	□
Are transportation companies selected with consideration of the procedures companies have in place to safeguard the security of product/animals being shipped?	□	□	□
Are transportation companies selected with consideration of background checks conducted on drivers and other employees who have access to product/animals?	□	□	□
Are ingredient suppliers selected with consideration of food security measures implemented by the suppliers?	□	□	□
Are vendors of compressed gas selected with consideration of food security measures implemented by vendors?	□	□	□
Are vendors of packaging materials and labels selected with consideration of food security measures implemented by vendors?	□	□	□

18. Does this establishment allow returned goods, including returns of U.S. exported products, to enter the plant?
    □ Yes
    □ No [GO TO QUESTION 20]

19. Which of the following security procedures does this establishment have in place for returned goods? *(Check "Yes" or "No" for each procedure.)*

	Yes	No
Are all returned goods examined for evidence of possible tampering before salvage or use in rework?	□	□
Are records maintained of returned goods used in rework?	□	□
Are returned goods reworked/examined at a separate designated location in the establishment to prevent potential cross-contamination of products?	□	□
Does the establishment follow the procedures outlined in FSIS Directive 9010.1 for return of U.S. exported products? http://www.fsis.usda.gov/oppde/rdad/fsisdirectives/9010-1.pdf	□	□

VII. WATER AND ICE SECURITY

Visit http://cfpub.epa.gov/safewater/watersecurity/index.cfm and www.epa.gov/region1/eco/drinkwater/pdfs/drinkingH2Ofactsheet.pdf for guidance material from the U.S. Environmental Protection Agency, Water Security.

20. Which of the following security procedures does this establishment have in place for its water and ice supply? *(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable.)*

	Yes	No	N/A
Is access to water wells restricted? (e.g., by locked door/gate or limiting access to designated employees)	□	□	□
Is access to ice-making equipment restricted?	□	□	□
Is access to ice storage facilities restricted?	□	□	□
Is access to storage tanks for potable water restricted?	□	□	□
Is access to water reuse systems restricted?	□	□	□
Are *potable* water lines periodically inspected for possible tampering? (i.e., visual inspection for physical integrity of infrastructure etc.)?	□	□	□
Are *non-potable* water lines inspected for possible tampering (i.e., visual inspection for physical integrity of infrastructure, connection to potable lines, etc.)?	□	□	□
Have arrangements been made with local health officials to ensure immediate notification of the plant if the potability of the public water supply is compromised?	□	□	□

VIII. MAIL HANDLING SECURITY

21. Which of the following security procedures does this establishment have in place to ensure mail handling security?

	Yes	No	N/A
Is mail handling activity conducted in a separate room or facility away from in-plant food production/processing operations?	□	□	□
Are mail-handlers trained to recognize and handle suspicious pieces of mail using U.S. Postal Service guidelines?	□	□	□
http://www.usps.com/news/2001/press/serviceupdates.htm			

IX. PERSONNEL SECURITY

22. Which of the following security procedures does this establishment have in place for ensuring that establishment personnel adhere to the security requirements?
(Check "Yes" or "No" for each procedure, or "N/A" if the procedure is not applicable [e.g., the establishment does not use contractors].)

	Yes	No	N/A
Are background checks or selective background checks conducted for new permanent staff who will be working in sensitive operations prior to hiring?	□	□	□
Are background checks or selective background checks conducted for workers in sensitive operations for new temporary, seasonal, and contract employees prior to hiring?	□	□	□

	Yes	No	N/A
Do all plant employees receive training on security procedures as part of their orientation training?	□	□	□
Are procedures in place to ensure positive identification/recognition of all establishment employees?	□	□	□
Are identification procedures in place to ensure the positive identification/recognition for temporary employees and contractors (including construction workers, cleaning crews, and truck drivers) in the establishment?	□	□	□
Are procedures in place to screen employees entering the plant during *working* hours?	□	□	□
Are procedures in place to screen entry of employees into the plant during *non-working* hours?	□	□	□
Are procedures in place to screen the entry of contractors into the plant during *working* hours?	□	□	□
Are procedures in place to screen entry of employees into the plant during *non-working* hours?	□	□	□
Are procedures in place to restrict temporary employees and contractors (including construction workers, cleaning crews, and truck drivers) to areas of plant relevant to their work?	□	□	□
Are procedures in place to ensure clear identification of personnel with their specific functions/assignments (e.g., colored garb)?	□	□	□
Is an updated shift roster, i.e., who is absent, who the replacements are, and when new employees are being integrated into the workforce, distributed to supervisors at the start of each shift?	□	□	□
Is a policy in place on what personal items may and may not be allowed inside the plant and within production areas?	□	□	□
Are announced and unannounced inspections of employees' lockers conducted?	□	□	□
Are employees and/or visitors restricted on what they can bring (cameras, etc.) into plant?	□	□	□
Are employees prohibited from removing company-provided clothing or protective gear from the premises?	□	□	□

APPENDIX—LIST OF RESOURCES

These resources contain security guidelines applicable to multiple sections of the checklist that establishments can adopt to enhance their capabilities to prevent intentional product tampering and to respond to threats or actual incidents of intentional product tampering. Additional resources with guidelines that apply only to specific sections are shown at appropriate sections throughout the document for easy access and reference.

FSIS Model Food Security Plans
http://www.fsis.usda.gov/Food_Security_&_Emergency_Preparedness/Security_Guidelines/index.asp#industry

FSIS "Security Guidelines for Food Processors"
http://www.fsis.usda.gov/oa/topics/SecurityGuide.pdf

World Health Organization (WHO) — "Terrorist Threats to Food — Guidelines for Establishing and Strengthening Prevention and Response Systems" (ISBN 92 4 154584 4)
http://www.who.int/foodsafety/publications/general/terrorism/en/

U. S. Food and Drug Administration (FDA) — "Food Security, Processors, and Transporters; Food Security Preventive Measures Guidance"
http://www.cfsan.fda.gov/~dms/secguid6.html

U.S. Food and Drug Administration (FDA)—"Retail Food Stores and Food Service Establishments; Food Security Preventive Measures Guidance"
http://www.cfsan.fda.gov/~dms/secgui11.html

Center for Disease Control and Prevention (CDC), National Institute of Occupational Safety and Health (NIOSH) —"Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks"
http://www.cdc.gov/niosh/bldvent/2002-139.html

USDA, Food and Nutrition Service (FNS) "A Biosecurity Checklist for Food Service Programs, Developing a Biosecurity Management Plan"
http://schoolmeals.nal.usda.gov/Safety/FNSFoodSafety.html

Canadian Food Inspection Agency (CFIA)—"Suggestions for Improving Security"
http://www.inspection.gc.ca/english/ops/secur/protrae.shtml

Center for Infectious Disease Research and Policy (CIDRAP), Academic Health Center, University of Minnesota
http://www.cidrap.umn.edu/cidrap/content/biosecurity/food-biosec/guidelines

County of San Diego, Department of Environmental Health, "Guidelines for Food Safety and Security"
http://www.sdcounty.ca.gov/deh/fhd/pdf/food_safety_security_217.pdf

SECURITY GUIDELINES FOR AMERICAN ENTERPRISES ABROAD

Overseas Security Advisory Council

INTRODUCTION

This appendix is a compilation of security guidelines for American private sector executives operating outside the United States. This guidance is the product of many years of experience by a cross section of American security practitioners from both the public and private sectors. Obviously, the implementation should be consistent with the level of risk in the country where you conduct business. For the most part the guidelines are for protection in high threat areas. It is recognized that the level of risk varies from country to country and time to so that you may need to choose among the suggested options or apply the concepts in a manner modified to meet your needs. Since levels of risk can change very rapidly, it is advisable to continuously monitor factors that may impact the risk level. Security precautions must be flexible and dynamic to respond effectively to changing risks. A static, inflexible security posture will almost certainly result in a lack of preparedness or unnecessary expense.

The Department of State has three threat assessment designators: High, Medium, and Low. One of these three threat designators is applied to each country where the United States has diplomatic representation. Threat assessment information is available to the American business community in countries where the United States has diplomatic representation through the Regional Security Officer or Post Security Officer at the nearest U.S. diplomatic post, i.e. Embassy or Consulate. The level assigned to a particular country is determined by an analysis of the political, terrorist, and criminal environment of that country. It is reviewed quarterly by the Department of State and changed when appropriate.

A High Threat country is one where the threat is serious and forced entries and assaults on residents are common, or where an active terrorist threat exists. A Medium Threat country is one where the threat is moderate, with some forced entries and assaults on residents occurring, or where the area has the potential for terrorist activity. A Low Threat country is one where the threat is minimal and forced entry of residences and assault of occupants is not common, and there is no known terrorist threat.

For emphasis again, the guidelines set forth in this publication are generally most appropriate for High Threat areas. One will probably want to moderate them for applications where the risk is lower; or where other considerations preclude their implementation at the level discussed here. In many situations, professional technical security assistance will be required.

These guidelines emphasize site selection and operational security. Appendices I and II are checklists which will help you determine your security needs.

SITE SELECTION GUIDELINES

Need for Security Criteria

From a security point of view, proper site selection is the most important initial step to provide adequate protection. It is the intent of this appendix to bring to the attention of all responsible personnel the wide range of security matters that should be addressed and integrated into the site selection process for new office buildings and existing buildings.

Because of car bombings there are new criteria for site selection on a worldwide basis. Regardless of the geographic process, thereby preparing for what might happen during the life of the building or its occupancy. We have all seen how quickly a benign security situation can evolve into a significant threat to facilities. It is only prudent to incorporate adequate security measures based on an evaluation of the existing threat and the potential for a higher future threat level to protect your employees and visitors for the long term. It will be evident from the factors highlighted that security considerations will impact on operational matters. The implication of this fact may be greater in some geographic regions than in others and will certainly affect some more seriously than others. Where this is the case, it is incumbent on all interested parties to evaluate potential damage while engaged in the site selection process and balance it against security requirements. If, in high threat areas, many of the suggested key criteria cannot be met the firm should consider choosing another, more secure location.

Everyone involved in site selections should be aware of the following suggested criteria for facilities.

New Office Building

Topography

Site ideally should be situated at the high point, if any, of a land tract, which makes it less vulnerable to weapons fire, makes egress/ingress more difficult and easier to detect or observe any intrusions.

Siting

Site should be located away from main thoroughfares and provide for the following:

- 100 feet minimum setback from the building to perimeter walls and vehicular entrances to the building.
- Sufficient parking space for personnel outside the compound in a secure area within sight of the building, preferably, immediately adjacent to the compound.

- Sufficient parking space for visitors near the site but not on the site itself.
- Sufficient space to allow for the construction of a vehicular security control checkpoint (lock-type system), which would allow vehicles to be searched, if deemed necessary, and cleared without providing direct access to the site.
- Sufficient space to allow for the construction of a pedestrian security control checkpoint (gatehouse/booth) to check identification, conduct a package check or parcel inspection or carry out visitor processing before the pedestrian is allowed further access to the site. If a need for a thorough check of purses and briefcases, as well as items carried on a person may be required, sufficient space for a Walk-Through Metal Detector (WTMD) should be considered. Walking through a WTMD is less intrusive than a personal search or even one conducted with a hand-held detector.
- Sufficient space for construction of a 9-foot outer perimeter barrier or wall.

Environmental Considerations

Site should be located in a semi-residential, semi-commercial area where local vehicular traffic flow patterns do not impede access to or from the site.

Existing Office Building

The following security considerations for high-rise buildings are listed in order of preference as the availability of local facilities dictate:

- A detached (free-standing) building and site entirely occupied and controlled by you.
- A semidetached office building that is entirely occupied by you.
- A nondetached office building that is entirely occupied and controlled by you.
- A detached (free-standing) office building in which the uppermost floors are entirely occupied and controlled by you.
- A semidetached office building in which the uppermost floors are entirely occupied and controlled by you.
- A nondetached office building in which the uppermost floors are entirely occupied and controlled by you.
- A detached (free-standing) office building in which the central floors are entirely occupied and controlled by you.
- A semidetached office building in which the central floors are entirely occupied and controlled by you.
- A nondetached office building in which the central floors are entirely occupied and controlled by you.
- A detached (free-standing) office building in which some floors are occupied and controlled by you.
- A semidetached office building in which some floors are occupied and controlled by you.

- A nondetached office building in which some floors are occupied and controlled by you.

Common Requirements

Both new and existing office buildings should be capable of accommodating these security items:

- Floor load capacity must be able to maintain the additional weight of public access control (PAC) equipment (ballistic doors, walls, windows), security containers, and disintegrators and shredders, if needed.
- Exterior walls must be smooth shell, sturdy, and protected to a height of 16 feet to prevent forced entry.
- Building must be conducive to grilling or eliminating all windows below 16 feet.

The previously listed criteria should be adopted to provide satisfactory protection for employees and visitors. If the site is found to be deficient in some areas, attempt to resolve those deficiencies by instituting security measures that will negate the deficiencies. Professional security and/or engineering assistance should be considered to address unique situations.

At a minimum, the following general security measures should be incorporated into planning designs: perimeter controls, grillwork, and shatter-resistant film for windows, public access controls, package search and check, secured area, provisions for emergency egress, and emergency alarms and emergency power.

Standards of Design for Site and Building Security

This section establishes the minimum physical security standards to be incorporated in the design of facilities.

The intent is to provide protection for assets, personnel, property, and customers; ensure that consistent security measures are used at various locations; and ensure design integrity and compatibility of all elements of security with the architecture of the site.

Labor-saving and state-of-the-art security system components and assemblies should be used in all U.S. activities operating overseas, provided they can be maintained locally and there are spare parts available locally.

For manufacturing plant and laboratory facilities, security equipment such as closed-circuit television (CCTV) cameras and monitors, intercoms, card readers, and special glass protection, should be considered. Special care should be taken to verify the vendor's references, especially as they pertain to the quality of alarms, a visit should be made to the central station to observe the professionalism of the operation. Design, purchase, and installation should be coordinated through your architect. Bear in mind, and make provisions for, the cost of maintenance on your security equipment. In some locations overseas, security equipment may be less expensive and more reliable than guards who receive relatively low pay and little training.

Security Design Objectives

In designing business or activity sites, roadways, buildings, and interior space, the following functional security objectives should be achieved:

- Physical and psychological boundaries (signs, closed doors, etc.) should establish four areas with increasing security controls beginning at the property boundaries. The areas are defined as:
    - perimeter—property boundaries;
    - exterior—lobbies/docks;
    - interior—employee space; and
    - restricted—laboratories, computer rooms, etc.
- Vehicular traffic signs should clearly designate the separate entrances for trucks/deliveries and visitors and employee vehicles. Where feasible control points should be provided near the site boundaries. Sidewalks should channel pedestrians toward controlled lobbies and entrances.
- Avoid having unsecured areas where there is no one nearby with responsibility for the function of the areas.

EXTERIOR PROTECTION

Perimeter Security

Walls, Fences, Berms, etc.

The overall design for perimeter security should consider using natural barriers, fencing, landscaping, or other physical or psychological boundaries to demonstrate a security presence to all site visitors.

If the threat is considered to be high at free-standing facilities, there should be a smooth faced perimeter wall or combination wall/fence, a minimum of 9 feet tall and extending 3 feet below grade. The wall or fence may be constructed of stone, masonry, concrete, chain link, or steel grillwork. However, if space limitations and local conditions dictate the need, any newly constructed wall should be designed to prevent vehicle penetration, and should use a reinforced concrete foundation wall, 18 inches thick with an additional 1-1/2 inches of concrete covering on each side of the steel reinforcement, and extending 36 inches above the grade. This type of wall is designed to support three wall toppings: masonry, concrete, or steel picket fencing. The toppings should be securely anchored into the foundation wall. If a picket fence is used instead of a wall, the upright supports should be spaced at least 9 feet apart so that the fence, if knocked down, can not be used as a ladder. In addition, intrusion alert systems can be used to enhance perimeter security.

In cases where the above standards of construction are neither feasible, fiscally prudent, nor required by the threat, alternative methods offering comparable protection can be used. These alternatives should maximize the use of locally available materials and conditions to take advantage of existing terrain features or by the creative use of earth berms and landscaping techniques such as concrete planters.

Inside the perimeter barrier, the building should be set back on the property to provide maximum distance from that portion of the perimeter barrier which is accessible by vehicle. The desirable distance of the setback is at least 100 feet depending on the bomb resistance provided by the barrier.

At facilities with less than optimum barriers, or at locations where the terrorist threat or building location increases the vulnerability to vehicular attack, bollards[1] or cement planters can be used to strengthen the perimeter boundary. At walled or fenced facilities with insufficient setback, bollards or planters can be installed outside the perimeter to increase the setback of the buildings.

(In any event, whether at a walled facility or a nonwalled one as discussed below, the design and placement of bollards or other antivehicular devices should be considered in the early planning stages. It would prevent having impenetrable gates connected by easily penetrated walls, or necessitate relocating because local authorities forbid the construction of required barriers.)

Nonwalled Facilities Barriers

In locations without perimeter wall protection, buildings should be protected with bollards, cement planters, or any other perimeter protection device. Such devices should be placed in a manner as to allow the maximum distance between the building and the roadway and/or vehicle access area. They should be positioned to impede vehicular access to lobbies and other glassed areas that could be penetrated by a vehicle (i.e., low or no curb, glass wall or door structure between lobby and driveway). Driveways should be designed and constructed to minimize or preclude high-speed vehicular approaches to lobbies and glassed areas. (There may be local ordinances that make placement of these devices illegal or ineffective.)

A positive and concerted effort should be made to contact local host country law enforcement or governmental authorities and request that they prohibit, restrict, or impede motor vehicles from parking, stopping, or loading in front of the facility.

In high threat locations, if local conditions or government officials prohibit antivehicular perimeter security measures and your business is either the sole occupant of the building or located on the first or second floor, you should consider relocating to more secure facilities.

Building Exterior

Facade

The building exterior should be a sheer/smooth shell, devoid of footholds, decorative lattice work, ledges, or balconies. The building facade should be protected to a height of 16 feet to prevent access by intruders using basic handtools. The use of glass on the building facade should be kept to an absolute minimum, only being used for standard size or smaller windows and, possibly, main entrance doors. All glass should be protected by plastic film. Consider the use of lexan or other polycarbonate as alternatives to glass where practical.

External Doors

Local fire codes may impact on the guidance presented here. As decisions are made on these issues, local fire codes will have to be considered.

Main entrance doors may be either transparent or opaque and constructed of wood, metal, or glass. The main entrance door should be equipped with a double-cylinder dead bolt and additionally secured with crossbar or sliding dead bolts attached vertically to the top and bottom of each leaf. All doors, including interior doors, should be installed to take advantage of the doorframe strength by having the doors open toward the attack side.

All other external doors should be opaque hollow metal fire doors with no external hardware. These external doors should be single doors unless used for delivery and loading purposes.

Should double doors be required, they should be equipped with two sliding dead bolts on the active leaf and two sliding dead bolts on the inactive leaf vertically installed on the top and bottom of the doors. A local alarmed panic bar and a 180-degree peephole viewing device should be installed on the active leaf.

All external doors leading to crawl spaces or basements must be securely padlocked and regularly inspected for tampering.

Windows

The interior side of all glass surfaces should be covered with a protective plastic film that meets or exceeds the manufacturer's specifications for shatter-resistant protective film. A good standard is 4-millimeter thickness for all protective film applications. This film will keep glass shards to a minimum in the event of an explosion or if objects are thrown through the window.

Grillwork should be installed on all exterior windows and air-conditioning units that are within 16 feet of grade or are accessible from roofs, balconies, etc. The rule of thumb here is to cover all openings in excess of 100 square inches if the smallest dimension is 6 inches or larger.

Grillwork should be constructed of 1/2 inch diameter or greater steel rebar, anchored or imbedded (not bolted) into the window frame or surrounding masonry to a depth of 3 inches. Grillwork should be installed horizontally and vertically on center at no more than 8 inch intervals. However, grillwork installed in exterior window frames within the secure area should be spaced 5 inches on center, horizontally and vertically, and anchored in the manner described previously. Decorative grillwork patterns can be used for aesthetic purposes.

Grillwork that is covering windows designated as necessary for emergency escape should be hinged for easy egress. All hinged grillwork should be secured with a key operated security padlock. The key should be maintained on a cup hook in close proximity of the hinged grille, but out of reach of an intruder. These emergency escape windows should not be used in planning for fire evacuations.

Roof

The roof should be constructed of fire-resistant material. All hatches and doors leading to the roof should be securely locked with dead-bolt locks. Security measures such as barbed, concertina or tape security wire, broken glass, and walls or fences may be used to prevent access from nearby trees and/or adjoining roofs.

Vehicular Entrance and Controls

Vehicular Entrance

Vehicular entry-exit points should be kept to a minimum. Ideally, to maximize traffic flow and security, only two regularly used vehicular entry-exit points are necessary. Both should be similarly constructed and monitored. The use of one would be limited to employees' cars, while the other would be used by visitors and delivery vehicles. Depending on the size and nature of the facility, a gate for emergency vehicular and pedestrian egress should be installed at a location that is easily and safely accessible by employees. Emergency gates should be securely locked and periodically checked. All entry-exit points should be secured with a heavy duty sliding steel, iron, or heavily braced chain link gate equipped with a heavy locking device.

The primary gate should be electrically operated (with a manual back-up by a security officer situated in an adjacent booth). The gate at the vehicle entrance should be positioned to avoid a long straight approach to force approaching vehicles to slow down before reaching the gate. The general technique employed is to require a sharp turn immediately in front of the gate.

In addition to the gate, and whenever justifiable, a vehicular arrest system can be installed. An appropriate vehicle arrest system, whether active, a piece of equipment designed to stop vehicles in their tracks, or passive, a dense mass, will be able to stop or instantly disable a vehicle with a minimum gross weight of 15,000 pounds traveling 50 miles per hour.

Vehicular Control

General. All facilities should have some method of vehicle access control. Primary road entrances to all major plant, laboratory, and office locations should have a vehicle control facility capable of remote operation by security personnel with automated systems.

- At smaller facilities, vehicle access control may be provided by badge-activated gates, manual swing gates, etc.
- Site security should be able to close all secondary road entrances thereby limiting access to the primary entrance. Lighting and turn space should be provided as appropriate.

Control Features. Primary perimeter entrances to a facility should have a booth for security personnel during peak traffic periods and automated systems for remote operations during other periods.

Capabilities are:

- Electrically-operated gates to be activated by security personnel at either the booth or security control center or by a badge reader located in a convenient location for a driver;
- CCTV with the capability of displaying full-facial features of a driver and vehicle characteristics on the monitor at security control center;
- An intercom system located in a convenient location for a driver to communicate with the gatehouse and security control center;
- Bollards or other elements to protect the security booth and gates against car crash;
- Sensors to activate the gate, detect vehicles approaching and departing the gate, activate a CCTV monitor displaying the gate, sound an audio alert in the security control center;
- Lighting to illuminate the gate area and approaches to a higher level than surrounding areas;
- Signs to instruct visitors and to post property as required;
- Road surfaces to enable queuing, turnaround, and parking;
- Vehicle bypass control (i.e., gate extensions), low and dense shrubbery, fences, and walls.

Booth Construction and Operation

As noted previously, at the perimeter vehicular entry-exit a security officer booth should be constructed to control access. (At facilities not having perimeter walls, the security officer booth should be installed immediately inside the facility foyer.)

If justified by the threat level the security officer booth should be completely protected with reinforced concrete, walls, ballistic doors, and windows. The booth should be equipped with a security officer duress alarm and intercom system, both annunciating at the facility receptionist and security officer's office. This security officer would also be responsible for complete operation of the vehicle gate. If necessary, package inspection and visitor screening may be conducted just outside of the booth by an unarmed security officer equipped with walk-through and handheld metal detectors. Provisions for the environmental comfort should be considered when designing the booth.

Parking

General. Security should be considered in the location and arrangement of parking lots. Pedestrians leaving parking lots should be channeled toward a limited number of building entrances.

All parking facilities should have an emergency communication system (intercom, telephones, etc.) installed at strategic locations to provide emergency communications directly to Security.

Parking lots should be provided with CCTV cameras capable of displaying and videotaping lot activity on a monitor in the security control center. Lighting must be of adequate level and direction to support cameras while, at the same time, giving consideration to energy efficiency and local environmental concerns.

If possible, parking on streets directly adjacent to the building should be forbidden. Wherever justifiable given the threat profile of your company, there should be no underground parking areas in the neither building basement nor ground-level parking under building overhangs.

Within Perimeter Walls/Fences. All parking within perimeter walls or fences should be restricted to employees, with spaces limited to an area as far from the building as possible. Parking for patrons and visitors, except for predesignated VIP visitors, should be restricted to outside of the perimeter wall/fences.

Garages. For those buildings having an integral parking garage or structure, a complete system for vehicle control should be provided. CCTV surveillance should be provided for employee safety and building security. If the threat of car bombing is extant, consideration must be given to prohibiting parking in the building.

Access from the garage or parking structure into the building should be limited, secure, well lighted, and have no places of concealment. Elevators, stairs, and connecting bridges serving the garage or parking structure should discharge into a staffed or fully monitored area. Convex mirrors should be mounted outside the garage elevators to reflect the area adjacent to the door openings.

Exterior Lighting

Exterior lighting should illuminate all facility entrances and exits in addition to parking areas, perimeter walls, gates, courtyards, garden areas, and shrubbery rows.

Lighting of building exterior and walkways should be provided where required for employee safety and security. Regarding building facades, there should be a capability to illuminate them 100% to a height of at least 6 feet.

Although sodium vapor lights are considered optimum for security purposes, the use of incandescent and florescent light fixtures is adequate. Exterior fixtures should be protected with grillwork when theft or vandalism have been identified as a problem.

For leased buildings, landlord approval of exterior lighting design requirements should be included in lease agreements.

Building Access

Building Entrances

The number of building entrances should be minimized, relative to the site, building layout, and functional requirements. A single off-hours entrance near the security control center is desirable. At large sites, additional secured entrances should be considered with provisions for monitoring and control.

Door Security Requirements

- All employee entrance doors should permit installation of controlled access system hardware. The doors, jambs, hinges and locks must be designed to resist forced entry (e.g., spreading of door frames, accessing panic hardware, shimming bolts and/or latches, fixed hinge pins). Don't forget handicap requirements when applicable.
- Minimum requirement for lock cylinders are "6-pin" pin-tumbler-type. Locks with removable core cylinders to permit periodic changing of the locking mechanism should be used.
- All exterior doors should have alarm sensors to detect unauthorized openings.
- Doors designed specifically for emergency exits need to have an alarm that is audible at the door with an additional annunciation at the security control center. These doors should have no exterior hardware on them.

Window Precautions

- For protection, large showroom type plate glass and small operable windows on the ground floor should be avoided. If, however, these types of windows are used and the building is located in a high-risk area, special consideration should be given to the use of locking and alarm devices, laminated glass, film, or polycarbonate glazing.
- For personnel protection, all windows should have shatter-resistant film.

- (For a more extensive discussion of windows and how to secure them, as well as guidance for securing windows which may be used for emergency exit, see “Windows” on page 639).

Lobby. Main entrances to buildings should have space for a receptionist during the day and a security officer at night. The security control center should be located adjacent to the main entrance lobby and should be surrounded by professionally designed protective materials.

The lobby-reception area should be a single, self-sufficient building entrance. Telephones and rest rooms to meet the needs of the public should be provided in this area without requiring entry into interior space. Rest rooms should be kept locked in high-threat environments and access controlled by the receptionist.

Consistent with existing risk level, the receptionist should not be allowed to accept small parcel or courier deliveries routinely unless they are expected by addressee.

Other Building Access Points

Other less obvious points of building entry, such as grilles, grating, manhole covers, areaways, utility tunnels, mechanical wall, and roof penetrations should be protected to impede and/or prevent entry into the building.

Permanent exterior stairs or ladders from the ground floor to the roof should not be used, nor should the building facade allow a person to climb up unaided. Exterior fire escapes should be retractable and secured in the up position.

Construction Activities

Landscaping and other outside architectural and/or aesthetic features should minimize creating any area that could conceal a person in close proximity to walkways, connecting links, buildings, and recreational spaces.

Landscaping design should include CCTV surveillance of building approaches and parking areas.

Landscape plantings around building perimeters need to be located at a minimum of 4 feet from the building wall to prevent concealing of people or objects.

INTERIOR PROTECTION

Building Layout

Building space can be divided into three categories: public areas, interior areas, and security or restricted areas requiring special security measures. These areas should be separated from one another within the building with a limited number of controlled passage points between the areas. "Controlled" in this context can allow or deny passage by any means deemed necessary (i.e., locks, security officers, etc.).

Corridors, stairwells, and other accessible areas should be arranged to avoid places for concealment.

Generally, restricted space should be located above the ground-floor level, away from exterior walls, and away from hazardous operations. Access to restricted space should be allowed only from interior space and not from exterior or public areas. Exit routes for normal or emergency egress should not transit restricted or security space.

Walls and Partitions

Public space should be separated from interior space and restricted space by slab-to-slab partitions. When the area above a hung ceiling is used as a common air return, provide appropriate modifications to walls or install alarm sensors. In shared occupancy buildings, space should be separated by slab-to-slab construction or as described previously.

Doors

Normally, interior doors do not require special features or provisions for locking.

In shared occupancy buildings, every door leading to interior space should be considered an exterior door and designed with an appropriate degree of security.

Stairway doors located in multitenant buildings must be secured from the stairwell side (local fire regulations permitting) and always operable from the office side. In the event that code prevents these doors from being secured, the floor plan should be altered to provide security to your space.

Emergency exit doors that are designed specifically for that purpose should be equipped with a local audible alarm at the door and a signal at the monitoring location.

Doors to restricted access areas should be designed to resist intrusion and accommodate controlled-access hardware and alarms.

Doors on building equipment and utility rooms, electric closets, and telephone rooms should be provided with locks having a removable core, as is provided on exterior doors. As a minimum requirement, provide 6-pin tumbler locks.

For safety reasons, door hardware on secured interior doors should permit exit by means of a single knob or panic bar.

Other Public Areas

The design of public areas should prevent concealment of unauthorized personnel and/or objects.

Ceilings in lobbies, rest rooms, and similar public areas should be made inaccessible with securely fastened or locked access panels installed where necessary to service equipment.

Public rest rooms and elevator lobbies in shared occupancy buildings should have ceilings that satisfy your security requirements.

Special Storage Requirements

Building vaults or metal safes may be required to protect cash or negotiable documents, precious metals, classified materials, etc. Vault construction should be made of reinforced concrete or masonry and be resistant to fire damage. Steel vault doors are available with various fire-related and security penetration classifications.

Elevators

All elevators should have emergency communications and emergency lighting. In shared occupancy buildings, elevators traveling to your interior space should be equipped with badge readers or other controls to prohibit unauthorized persons from direct entry into your interior space. If this is not feasible, a guard, receptionist or other means of access control may be necessary at each entry point.

Cable Runs

All cable termination points, terminal blocks, and/or junction boxes should be within your space. Where practical, enclose cable runs in steel conduit.

Cables passing through space that you do not control should be continuous and installed in conduit. You might even want to install an alarm in the conduit. Junction boxes should be minimized and fittings spot welded when warranted.

Security Monitoring

Security Control Center

If you have a security control center, it should have adequate space for security personnel and their equipment. Additional office space for technicians and managers should be available adjacent to the control center.

Your security control center should provide a fully integrated console designed to optimize the operator's ability to receive and evaluate security information and initiate appropriate response actions for (1) access control, (2) CCTV, (3) life safety, (4) intrusion and panic alarm, (5) communications, and (6) fully zoned public address system control.

The control center should have emergency power and convenient toilet facilities. Lighting should avoid glare on TV monitors and computer terminals. Sound-absorbing materials should be used on floors, walls, and ceilings. All security power should be backed up by an emergency electrical system.

The control center should be protected to the same degree as the most secure area it monitors.

Controlled Access System

This type of system, if used, should include the computer hardware, monitoring station terminals, sensors, badge readers, door control devices, and the necessary communication links (leased line, digital dialer, or radio transmission) to the computer.

In addition to the normal designated access control system's doors and/or gates, remote access control points should interface to the following systems: (1) CCTV, (2) intercom, and (3) door and/or gate release.

Alarm Systems

Sensors should be resistant to surreptitious bypass. Door contact monitor switches should be recessed wherever possible. Surface-mounted contact switches should have protective covers.

Intrusion and fire alarms for restricted areas should incorporate a backup battery power supply and be on circuits energized by normal and emergency generator power.

Control boxes, external bells, and junction boxes for all alarm systems should be secured with high-quality locks and electrically wired to cause an alarm if opened.

Alarm systems should be fully multiplexed in large installations. Alarm systems should interface with the computer-based security system and CCTV system.

Security sensors should individually register an audio-visual alarm (annunciator or computer, if provided) located at the security central monitoring location and alert the security officer. A single-CRT display should have a redundant printer or indicator light. A hard-wired audible alarm that meets common fire code standards should be activated with distinguishing characteristics for fire, intrusion, emergency exit, etc. All alarms ought to be locked in until reset manually.

Closed-Circuit TV (CCTV)

CCTV systems should permit the observation of multiple camera transmission images from one or more remote locations.

Switching equipment should be installed to permit the display of any camera on any designated monitor.

Hardware

To ensure total system reliability, only high quality security hardware should be integrated into the security system.

Stairwell Door Reentry System

In multitenant high-rise facilities, stairwell doors present a potential security problem. These doors must be continuously operable from the office side into the stairwells. Reentry should be controlled to permit only authorized access and prevent entrapment in the stairwell.

Reentry problems can be fixed if you provide locks on all stairwell doors except the doors leading to the first floor (lobby level) and approximately every fourth or fifth floor, or as required by local fire code requirements. Doors without these locks should be fitted with sensors to transmit alarms to the central security monitoring location and provide an audible alarm at the door location. Appropriate signs should be placed within the stairwells. Doors leading to roofs should be secured to the extent permitted by local fire code.

Special Functional Requirements

Facilities with unique functions may have special security requirements in addition to those stated in this booklet. These special requirements should be discussed with Corporate Security personnel or a security consultant. Typical areas with special requirements are product centers, parts distribution centers; sensitive parts storage facilities, customer centers, service exchange centers, etc.

PUBLIC ACCESS CONTROLS (PAC)

Security Officers and Watchmen

All facilities of any size in threatened locations should have manned 24 hour internal protection. Security Officers should be uniformed personnel and, if possible, placed under contract. They should be thoroughly trained, bilingual and have complete instructions in their native language clearly outlining their duties and responsibilities. These instructions should also be printed in English for the benefit of American supervisory personnel. If permitted by local law/customs, investigations or checks into the backgrounds of security officers should be conducted.

At facilities with a perimeter wall, there should be one 24 hour perimeter security officer post. If the facility maintains a separate vehicular entrance security officer post, such a post should be manned from 1 hour before to 1 hour after normal business hours and during special events. Security officers should be responsible for conducting package inspections, package check-in, and, if used, should operate the walk-through and hand-held metal detectors. Security officers should also be responsible for inspecting local and international mail delivered to the facility, both visually and with a hand-held metal detector before it is distributed. X-ray equipment for package inspection should be employed if the level of risk dictates.

At facilities with a perimeter guardhouse, the walk-through metal detector could be maintained and operated in an unsecured pass-through portion of the guardhouse. In addition, this security officer could also be responsible for conducting package inspections. When there is sufficient room to store packages at the guardhouse, checked packages should be stored here—new guardhouses should provide for such storage. If package storage at the guardhouse is not feasible, then it should be in shelves in the foyer under the direction of the foyer security officer or receptionist. Generally, security screening and package storage is carried out in the foyer.

Security Hardline

Office areas should be equipped with a "hardline" to provide physical protection from unregulated public access. Protection should be provided by a forced-entry-resistant hardline that meets ballistic protection standards. These standards can be obtained from your corporate personnel or a security consultant. When a security hardline for Public Access Control (PAC) is constructed, the following criteria should apply:

Walls

Walls comprising a PAC should be constructed of no less than 6 inches of reinforced concrete from slab to slab. The reinforcement should be of at least Number 5 rebar spaced 5 inches on center, horizontally and vertically, and anchored in both slabs. In existing buildings, the following are acceptable substitutions for 5-inch reinforced concrete hardlines:

- Solid masonry, 6 inches thick or greater, with reinforcing bars horizontally and vertically installed;
- Solid unreinforced masonry or brick, 8 inches thick or greater;
- Hollow masonry block, 4 to 8 inches thick with 1/4 inch steel backing;
- Solid masonry, at least 6 inches thick, with 1/4 inch steel backing;
- Fabricated ballistic steel wall, using two 1/4 inch layers of sheet steel separated by tubular steel studs;
- Reinforced concrete, less than 6 inches thick with 1/8 inch steel backing.

Security Doors

Either opaque or transparent security doors can be used for PAC doors. All doors should provide a 15 minute forced entry penetration delay. In addition, doors should be ballistic resistant.

The PAC door should be a local access control door, meaning a receptionist or security officer can remotely open the door.

Security Windows

Whenever a security window or teller-window is installed in the hardline, it should meet the 15 minute forced entry and standard ballistic resistance requirements.

PAC Entry Requirements

No visitor should be allowed to enter through the hardline without being visually identified by a security officer, receptionist, or other employee stationed behind the hardline. If the identity of the visitor cannot be established, the visitor must be escorted at all times while in the facility.

Alarms and Intercoms

A telephone intercom between the secure office area, the foyer security officer, and guardhouse should be installed. In facilities where deemed necessary, a central alarm and public address system should be installed to alert staff and patrons of an emergency situation. Where such a system is required, the primary control console should be located in the security control center. Keep in mind that alarms without emergency response plans may be wasted alarms. Design, implement, and practice emergency plans.

Secure Area

Every facility should be equipped with a secure area for immediate use in an emergency situation. This area is not intended to be used for prolonged periods of time. In the event of emergency, employees will vacate the premises as soon as possible. The secure area, therefore, is provided for the immediate congregation of employees at which time emergency exit plans would be implemented.

The secure area should be contained within the staff office area, behind the established hardline segregating offices from public access. An individual office will usually be designated as the secure area. Entrance into the secure area should be protected by a solid core wood or hollow metal door equipped with two sliding dead bolts.

Emergency egress from the secure area will be through an opaque 15 minute forced-entry-resistant door equipped with an alarmed panic bar or through a grilled window, hinged for emergency egress. The exit preferably will not be visible from the facility's front entrance.

EMERGENCY EXIT

All facilities should have a means of emergency escape aside from the secure area exit. Positioned appropriately throughout the building should be sufficient emergency exit points to accommodate normal facility occupancy.

All emergency doors should be hollow metal doors (fire doors where appropriate) equipped with alarmed emergency exit panic bars.

Emergency factors regarding windows are described on page 640.

COMMUNICATIONS

Communications Facilities

Satellite ground stations, microwave parabolic reflectors, and communications towers and supports should be located on rooftops, with limited access to the public. Where this is not possible, the equipment should be installed with fences and alarms. Closed circuit television (CCTV) with video recording capability should be considered and included where justified.

Communications

Telephone systems should incorporate an external direct line telephone link for security and life safety independent of the internal telephone network dedicated to the location. This line should feed into the secure area.

Communications considerations should provide radio transmission equipment for communications between security personnel.

Intercom systems should have the capacity to accommodate all remote access control points.

Systems Integration

Security systems in new buildings or buildings undergoing renovation should be installed with distributed wiring schemes that use local telecommunication closets as distribution points. This will provide expansion capability, future networking capability, ease of maintenance, and full function implementation of the security system. At a minimum, the communications link and interface between the sensor, output devices, and computers should include conduit, multiconductor twisted shielded cable and terminal cabinets. However, recent technology such as fiber-optic cables should be considered in planning the wiring distribution scheme. Data distribution and gathering closets used for security wiring must be secure. Where possible, integrate security wiring with other systems such as telephone, paging, energy management, etc. In every case, the design of the communications link should permit ready installation and interconnection of cameras, sensors, and other input-output devices. All life safety equipment and accessories should be Underwriters Laboratory (UL) approved.

Outlying facilities should link security systems to the nearest security control center. All new systems should be compatible with existing systems or the existing system should be replaced with the new system.

OFFICE SECURITY GUIDELINES

General Procedures

Any employee, but especially the executive, can be a target of terrorist or criminal tactics and forced entry, building occupation, kidnapping, sabotage, and even assassination. Executive offices can be protected against attacks.

The executive office should have a physical barrier such as electromagnetically operated doors, a silent trouble alarm button, with a signal terminating in the Plant Protection Department or at the secretary's desk, and close screening of visitors at the reception and security officer desks in the lobbies and again at the executive's office itself. Secretaries should not admit visitors unless positively screened in advance or known from previous visits. If the visitor is not known and/or not expected, he or she should not be admitted until satisfactory identification and a valid reason to be on site is established. In such instances, Security should be called and an officer asked to come to the scene until the visitor establishes a legitimate reason for being in the office. If the visitor cannot do so, the officer should be asked to escort the visitor out of the building.

Unusual telephone calls, particularly those in which the caller does not identify himself/herself or those in which it appears that the caller may be misrepresenting himself/herself, should not be put through to the executive. Note should be made of the circumstances involved (i.e., incoming line number, date and time, nature of call, name of caller). This information should then be provided to the Security Department for follow-up investigation.

Under no circumstances should an executive's secretary reveal to unknown callers the whereabouts of the executive, his/her home address, or telephone number.

The executive, when working alone in the evening, on weekends, or holidays, should advise Security how long he/she will be in the office and check out with Security when leaving.

Security in the Office

American enterprises, particularly those in foreign countries, have been and will continue to be the subject of controversial political and economic issues that can turn their executives and offices into targets for terrorists and criminal actions. Countermeasures against these acts can and should be implemented in the office environment. The following list describes some of the measures that may be useful in improving personal security and safety at the office.

- Avoid working alone late at night and on days when the remainder of the staff is absent.
- The office door should be locked when you vacate your office for any lengthy period, at night and on weekends. Do not permit the secretary to leave keys to the office or desk.

- There should be limited access to the executive office area.
- Arrange office interiors so that strange or foreign objects left in the room will be immediately recognized.
- Unescorted visitors should not be allowed admittance nor should workmen without proper identification and authorization.
- Implement a clean desk policy. Do not leave papers nor travel plans on desk tops unattended.
- Control publicity in high-risk areas. Avoid identification by photographs for news release. Maintain a low profile.
- Janitorial or maintenance activity in key offices and factory areas should be supervised by competent company employees.
- A fire extinguisher, first-aid kit, and oxygen bottle should be stored in the office area.
- The most effective physical security configuration is to have doors locked (from within) with one visitor access door to the office area.
- Where large numbers of employees are involved, use the identification badge system containing a photograph.

Advice for Secretaries

A secretary has close knowledge of schedules and company business. He/she should be instructed to maximize security, and the following precautionary measures should be reviewed with him/her:

- Be alert to strangers visiting the executive without an appointment and who are unknown to him/her.
- Be alert to strangers who loiter near the office.
- Do not reveal the executive's whereabouts to unknown callers. Even if the caller is known, the information should be on a need-to-know basis. As a standard policy, take a number where the caller can be contacted. Do not give out home telephone numbers or addresses.
- When receiving a threatening call, including a bomb threat, extortion threat, or from a mentally disturbed individual, remain calm and listen carefully. Each secretary and/or receptionist should have a threatening telephone call checklist which should be completed as soon as possible. A boiler-plate checklist is attached as Appendix III.
- Keep executive travel and managers' travel itineraries confidential. Strictly limit distribution to those with a need to know.
- Incinerate, disintegrate or shred notes, drafts, correspondence and any and all material which reveal an executive's travel plans, itineraries, home address and telephone number, invitations and responses thereto or any other data about his/her whereabouts, including information about past trips which could indicate habitual contacts and travel patterns. Do not place such material in trash cans.

- Observe caution when opening mail. A list of things to look for is included in Appendix IV. You should post this list in your mail handling facility. (All persons handling mail should be made aware of the aforementioned basic signs found in Appendix IV. The mail handlers should have available an established procedure in the event that any of the above signs are found. It is also important not to accept packages from strangers until satisfied with the individual's identity and the nature of the parcel.)

Precautions for All

Money, valuables, and important papers such as passports should not be kept in a your desk. Thefts will occur in all offices, even during working hours. Some will be solved, most could have been prevented. The following suggestions will decrease the chance of further thefts:

- Do not tempt thieves by leaving valuables or money unsecured.
- If sharing an office or suite of offices, stagger lunch hours and coffee breaks so that the office is occupied at all times.
- If the office must be left vacant, lock the door.
- Locate desks in a way that persons entering the office or suite can be observed.
- Follow a clean desk policy before leaving at night. Keep valuables and company documents in locked containers.
- Confirm work to be done or property to be removed by Maintenance, outside service personnel, or vendors.
- Do not "hide" keys to office furniture under flower pots, calendars, etc. Thieves know all the hiding places. Do not label keys except by code.

VEHICULAR AND TRAVEL SECURITY

Vehicle and Travel Security

Threats of terrorism and kidnapping are serious problems involving all aspects of security management; effective management dictates that available resources be used wisely and concentrated on security weak points. Terrorists are very quick to identify the security vulnerabilities of business, family, and pleasure travel. At their best, protection strategies dealing with vehicles and travel are perhaps the hardest to formulate, and the advantage tends to be with the terrorist. Current statistics indicate that the greatest danger from acts of terrorism occurs while the executive is traveling to or from the office and just before reaching his/her destination.

The inherent security problems of passenger vehicle travel are many. Vehicles are easily recognized by year, make, and model, and the trained terrorist can accurately assess any protection modifications and security devices. Using adequate resources, vehicles can be discreetly followed; therefore, making possible repeated dry runs of potential attacks with very low risk of detection. Under these conditions, different methods of attack can be formulated and tested until success is ensured. While traveling in a passenger vehicle, the executive has limited protection resources upon which to rely and often is dependent on fixed security manpower. This makes it easier for terrorist groups, which are geared to mobility, to ensure numerical superiority.

The attack potential against the executive in travel rests heavily on psychological instability and human weakness. The shock of surprise attack is greatest at points of changing surroundings, crossroads, and when entering or exiting vehicles. These are situations of constant change and points of activity where the executive has a tendency to be mentally off balance. Vehicles are often left in driveways, on streets, at service centers, and other isolated areas with no form of control or protection, allowing easy access to terrorists. Through illegal entry to the vehicle, the terrorist can gain a number of attack points; sabotage with the intent to maim and injure, sabotage with the intent of execution, and sabotage to ensure the success of future attacks. These psychological factors make the vehicle the ideal place to apply scare tactics, warnings, and gain initial control of the executive.

Even though travel problems provide the greatest number of security and psychological variables, there are actions and policies that can be developed to minimize the executive's risk and complicate the terrorist's plans. The basic travel policy can be divided into three areas: (1) Normal Travel Procedures, (2) Vehicle Equipment, and (3) Vehicle Defense Strategy. The following checklists will aid in formulating and evaluating an effective travel security policy.

Normal Travel Procedures Checklist

- The avoidance of routine times and patterns of travel by executives is the least expensive security strategy that can be utilized. The selection of the route should be at the discretion of the executive, not of the chauffeur. Always restrict travel plans to a need-to-know basis.
- Avoid driving in remote areas after dark and keep to established, well-traveled roads.
- In high-risk areas or when individuals are considered attractive targets, consideration should be given to executives and drivers being trained in antiterrorism strategy and defensive driving. Establish responsibilities and develop contingency plans.
- There should be a simple duress procedure established between the executive and drivers. Any oral or visual signal will suffice (i.e., something that the executive or driver says or does only if something is amiss).
- Never overload a vehicle, and all persons should wear seat belts.
- Always park vehicles in parking areas that are either locked or watched and never park overnight on the street. Before entering vehicles, check for signs of tampering.

- When using a taxi service, vary the company. Ensure that the identification photo on the license matches the driver. If uneasy for any reason, simply take another taxi.
- When attending social functions, go with others, if possible.
- Avoid driving close behind other vehicles, especially service trucks, and be aware of activities and road conditions two to three blocks ahead.
- Keep the ignition key separate and never leave the trunk key with parking or service attendants.
- Before each trip, the vehicle should be inspected to see that (1) the hood latch is secure, (2) the fender wells are empty, (3) the exhaust pipe is not blocked, (4) no one is in the back seat or on the floor, and (5) the gas tank is at least three quarters full.
- Establish a firm policy regarding the carrying and use of firearms. Local laws may prohibit firearms.

Vehicle Equipment Checklist

- The executive vehicle designed to meet the terrorist or criminal threat in a high threat area should be a hardtop model with the following special equipment: (1) inside hood latch, (2) locked gas caps, (3) inner escape latch on trunk, (4) steel-belted radial tires with inner tire devices that permit movement even with a flat tire, (5) radiator protection, (6) disk brakes, and (7) an anti-bomb bolt through the end of the exhaust pipe.
- Positive communications can be ensured with a two-way radio or a car telephone.
- It is recommended that the executive vehicle designed to meet the terrorist or criminal threat carry the following safety equipment: (1) fire extinguisher, (2) first-aid kit, (3) flashlight, (4) two spare tires, (5) large outside mirrors, and (6) a portable high-intensity spotlight.
- For additional protection, the vehicle should have an alarm system with an independent power source (an additional battery).

Vehicle Defense Strategy Checklist

- Always be alert to possible surveillance; if followed, drive to the nearest safe location, such as police stations, fire stations, or shopping center and ask for help. Carry a mini-cassette recorder in the car to dictate details of a suspect surveillance car such as color, make, model, license plate, description of occupants, etc. It is difficult to make such detailed notes while driving.
- Where feasible, drive in the inner lanes to keep from being forced to the curb.
- Beware of minor accidents that could block traffic in suspect areas; especially crossroads because they are preferred areas for terrorist or criminal activities as crossroads offer escape advantages.

- If a roadblock is encountered, use shoulder or curb (hit at 30-45 degree angle) to go around, or ram the terrorist or criminal-blocking vehicle. In all cases, do not stop and never allow the executive's vehicle to be boxed in with a loss of maneuverability.
- Blocking vehicles should be rammed in a nonengine area, at 45 degree, in low gear, and at a constant moderate speed. KNOCK THE BLOCKING VEHICLE OUT OF THE WAY.
- Whenever a target vehicle veers away from the terrorist vehicle, it gives adverse maneuvering room and presents a better target to gunfire.

Travel Security Suggestions

The following are general traveling security suggestions:

- Discuss travel plans on a need-to-know basis only. Telephone operators and secretaries should not advise callers and visitors when an executive is out of town on a trip.
- Remove company logos from luggage. Luggage identification tags should be of a type that allows the information on the tag to be covered. Use the business address on the tag.
- Do not leave valuables and/or sensitive documents in the hotel room.
- When sightseeing, observe basic security precautions and refrain from walking alone in known high-crime areas.
- Always have telephone change available and know how to use the phones. Learn key emergency phrases of the country to be able to ask for police, medical, etc.
- Joggers should carry identification.
- Men should carry wallets either in an inside jacket pocket or a front pants pocket, never in a hip pocket. The less money carried the better. Credit cards can be used for most purchases.
- The telephone numbers of the U.S. Embassy or U.S. Consulate, and company employee contact numbers should be carried with employees at all times.
- Always carry the appropriate documentation for the country being visited.
- When traveling, ask for a hotel room between the second and seventh floors. Most fire department equipment does not reach higher to effect rescue and ground floor rooms are more vulnerable to terrorist or criminal activity.
- American-type hotels usually offer a higher level of safety and security inasmuch as they offer smoke alarms, fire extinguishers, safety locks, hotel security, 24 hour operators, English-speaking personnel, safety deposit boxes, and normally will not divulge a guest's room number.
- Choose taxis carefully and at random. Be sure it is a licensed taxi. Do not use independent non-licensed operators.
- Be as inconspicuous as possible in dress, social activities, and amount of money spent on food, souvenirs, gifts, etc.

- Stay in or use VIP rooms or security zones when waiting in commercial airports abroad. Minimize the amount of time spent in airports.
- Confirm arrivals at destinations with office and/or family. Use an itinerary when traveling.
- When traveling internationally, keep all medicine in original containers and take a copy of the prescription.

VISITING PERSONNEL PROTECTION

General Principles

This chapter provides guidelines regarding security procedures to be implemented during visits of company executives. Guidelines for three levels of threat (minimal threat, moderate threat and high threat) are set forth below along with the factors which determine the level of threat that may exist.

These guidelines should be viewed as tools to assist in organizing and planning visits by company executives or other key personnel. Their implementation will reduce the executive's exposure to terrorist acts, criminal activity, and potential embarrassment.

Minimal Threat-Factors and Guidelines

Minimal Threat Factors

Factors which should be used by management in determining whether in view of the local security environment a minimal threat potential exists include the following:

- A stable local government;
- Effective law enforcement;
- No significant history of terrorist acts against multinational companies or their executives;
- No previous history of criminal or terrorist acts directed against company executives;
- No significant level of criminal activity (particularly violent crimes such as robbery, kidnapping, murder, and rape);
- No current adverse publicity against the company and no local group activity protesting company policies;
- Other risk factors applicable to the local environment.

Minimal Threat Guidelines

Security Coordination. A management-level employee should be assigned as security coordinator. The coordinator's responsibilities consist of implementing the established security guidelines, coordinating all other security aspects of the visit, and serving as the visitor's main contact.

The coordinator should be present at the airport, hotel, and events during arrivals and departures. He/she should ensure adequate security precautions are taken and be present at large public functions.

Air Travel

- Travel in corporate aircraft is preferable because contact with the general public is limited, but use of commercial airlines is an acceptable alternative provided the airline involved is not considered a likely terrorist target.
- When booking reservations, you should make no reference to the visitor's position.
- Personnel should be available at the airport to handle baggage and expedite customs clearances and local airport formalities, both on arrival and departure. A VIP room should be reserved at the airport for possible use in the event of a delayed departure by the aircraft.
- Time spent at the airport should be kept to a minimum. Public areas should be avoided, if at all possible.
- Use of public transportation to and from airports is not recommended.
- Distribution of travel itineraries should be restricted.

Aircraft Security. This section applies in the event that corporate aircraft are used.

- The hiring of contract security officers at major international airports to secure the corporate aircraft during stopovers is not necessary provided that the airport has a viable security system.
- The use of contract security officers on a 24 hour basis is necessary in the event that the corporate aircraft uses a remote airfield with limited operations and minimal security or is parked in a remote area of a major airport.

Local Transportation

- The use of public transportation such as taxis, buses, and subways is not recommended.
- A four-door sedan should be available for use throughout the visit. Care should be taken to ensure that the vehicle is unobtrusive, so as not to bring undue attention to the visitor. The chauffeur or driver, if used, should be bilingual and knowledgeable of the local area and routes to be traveled.

Accommodations

- Hotel reservations should be booked at a first class hotel located in a low-crime area. Hotel management need not be contacted to provide unusual security or other arrangements for the visitor. A low-key approach is essential to ensure anonymity. Reference to the company or the visitor's position should be avoided.

- Visitors should be preregistered to avoid being required to check in at the reception desk. The room key should be provided to the visitor immediately upon his or her arrival at the hotel or airport by personnel responsible for coordinating the visit.
- The guest room or suite should be located between the second and seventh floor of the hotel, preferably on a floor with a separate concierge. The room should be away from the public elevator lobby but near an emergency exit.
- Valuables should be stored in accordance with hotel safekeeping provisions.
- Use of a guesthouse or private residence is acceptable as long as it is not located in an isolated area.

Official Functions and Activities

- Coordinate all activities and visit sites before the visitor's attendance. The coordinator should obtain guest lists and detailed itineraries, determine emergency evacuation routes, and ascertain the purpose of the function.
- The coordinator should ensure that the function or activity does not subject the visitor to undue risk.
- Official company functions should be on an invitational basis and guests should be required to present their invitations at a reception desk staffed by company personnel before being granted access to the function. The receptionist should match the invitation to the guest list.

Liaison With Local Authorities. Prior to a visit by a VIP, you should make contact with the appropriate local authorities to advise them of the upcoming visit and to ascertain whether the current local security environment necessitates an upgraded security posture for the visit.

Background Data. An information packet should be prepared before the visit and presented to the executive upon his/her arrival. Information provided should include:

- Emergency telephone contact list, including company personnel (home and office numbers), hospital, police, fire, emergency services, and company doctor;
- Maps of the area;
- Detailed itinerary;
- Availability of company transportation;
- Brief review of current security situation including curfews, government-imposed restrictions, description of high-crime areas to be avoided, and other relevant factors; and
- Explanation of local currency (exchange rates and currency control laws or regulations).

Other

- Details of visits by VIPs should be considered company confidential and distribution limited on a need-to-know basis.
- Media coverage, unless requested by the visitor, is unwarranted.

Moderate Threat-Factors and Guidelines

Moderate Threat Factors

Factors which should be used by management in determining whether in view of the local security environment a moderate threat potential exists include the following:

- Stable local government;
- Effective law enforcement;
- Some history of terrorist attacks against multinational companies and/or their executives;
- No previous history of criminal or terrorist acts directed against company executives;
- Upswing in criminal activity, particularly violent crimes with some history of criminal kidnappings for financial gain;
- Some current adverse publicity against the company and potential for nonviolent groups to protest against company policies during the executive's visit.

Moderate Threat Guidelines

Unarmed Security Escort. In addition to the guidance set forth in "Minimal Threat Guidelines," an unarmed security escort should be used when a determination is made by management that a moderate threat exists.

High Threat-Factors and Guidelines

High Threat Factors

Factors which should be used by management in determining whether in view of the local security environment a high threat potential exists include the following:

- Unstable or unpopular local government, with terrorist groups actively attempting to bring about its overthrow;
- Ineffective or corrupt law enforcement agencies unable to reduce criminal activity and bring the terrorist problem under control;
- Significant history of terrorist attacks against multinational companies and/or their executives, including bombings, assassinations, and kidnappings;
- Recent history of criminal or terrorist acts or threats against company facilities and/or their executives;

- Widespread criminal activity reaching all elements of local society with emphasis on violent crimes;
- Considerable adverse publicity against company policies and organized local groups that have been leaning toward violence and are planning to protest company policies during the executive's visit;
- Other factors appropriate to the local environment. Asking the consulate regional security officer at the embassy is a good idea.

High Threat Guidelines

Recommendation Against Visit. High-threat potential means a significant risk to the well being of the executive. You should strongly recommend against a visit by the executive if a high risk exists. By definition, this category will apply to a limited number of locations, but might vary based on the local situation at a particular point in time. For example, a potential visit might be deemed a moderate risk one month and high risk another because of changes in the local environment.

Armed Protective Security Detail. If the executive cannot be dissuaded from visiting the high threat area, an armed protective security detail should be used.

Specific guidelines for high risk protective details are beyond the scope of this document because of the multiple and various considerations in organizing each individual protective detail. However, the use of trained security professionals is essential.

The items covered in "Minimal Threat Guidelines", will still have to be addressed when an armed protective detail is required. However, the manner in which relevant tasks are performed may be modified by guidelines issued in regard to the armed details. Some general guidelines are as follows:

- Professional bodyguards dressed in plainclothes and equipped with weapons and two-way radios should accompany the executive at all times. At least one bodyguard should remain in the direct vicinity of the executive whenever potential public contact is envisioned.
- Security personnel should conduct advance surveys of all sites to be visited and be on the scene throughout the executive's visit to the location.
- Security personnel should be assigned to the hotel or residence on a 24 hour basis to ensure that unauthorized individuals do not enter the room or suite. Cleaning staff should be escorted whenever they enter the accommodations. The room or suite should be periodically checked to ensure that contraband (such as a bomb) has not been introduced into the area.
- An escort car or cars should be used on all vehicular movements by the executive to provide a response capacity in the event of an attack or vehicular

mishap or breakdown. The escort car or cars should be staffed by at least two security professionals.

- The executive's vehicle should be driven by a security professional trained in evasive or defensive maneuvers. The vehicle should be inspected before use to ensure that explosive devices have not been installed on the vehicle or that the vehicle has not been otherwise tampered with by unauthorized individuals. Use of an armored car, if available, is recommended.
- Public exposure should be limited to the minimum necessary for the executive to complete his or her assignment.

Group Activities Guidelines

The exposure created by a number of executives gathering at a single location necessitates some degree of increased security. The following is a list of some general guidelines for use in such group activities:

- The suites should be inspected before occupancy to ensure that no contraband or unauthorized individuals are located in the rooms.
- Security should be provided for corporate aircraft overnighting at the local airport. Such security may be provided by off-duty uniformed and armed police officers or contract security guards.
- The hotel activity boards should make no reference to the company. Publicity and press coverage should be minimized. A low profile is strongly recommended. Anonymity is a powerful ally of a traveling executive.
- If possible, hotel guest rooms occupied by company personnel should be located in one section of the hotel. Consideration should be given to hiring a security officer to patrol the hallway in the vicinity of the guest rooms and function rooms during hours of darkness or even on a 24-hour basis.
- Access to functions should be controlled to prevent and unauthorized individual from gaining access to the meetings or functions. This can be handled by assigning a member of the meeting staff to serve as a receptionist outside the door. Access can be granted either by personal recognition or by checking identify cards.
- Information packets provided to participants should include the name and telephone number of the staff person responsible for security. Staff personnel should be provided with an emergency contact list, including the telephone numbers of the nearest hospital with an emergency room, ambulance service, police department, and fire department.
- Consideration should be given to leasing pagers to ensure that staff personnel can be rapidly contacted in the event of an emergency.
- Upon the conclusion of the meeting, staff personnel should inspect all guest rooms and function rooms to ensure that no documents, personal effects, or equipment have been left behind by participants.

NOTE

[1] A device constructed to protect against a ramming vehicle attack. They are deployed in lines around a perimeter for anti-ram protection, or to provide supplemental control of vehicle traffic through permanent checkpoints when other means are not practical or effective.

APPENDIX I: SECURITY SURVEY CHECKLIST

General, Preparatory Data

1. Site name, address, telephone number:
   Please fill in the name of the people holding the following positions:
   Manager
   Assistant Manager
   Human Resources Manager
   Person responsible for site security
   Number of Employees
   Area Covered/Office Size
   Operating Hours
   Function
2. Survey should include review of theft reports prepared by this site for an appropriate prior period. Where appropriate, has corrective action been taken?
   Do theft reports reflect patterns, trends, or particular problems at this location?
3. What does site management regard as the most prevalent or serious security problem?
4. Does the site maintain items of value, such as works of art, paintings, wall hangings, etc.?
5. What are the site's most valuable physical assets?
6. Does the location have an employees' handbook or manual or other means of enumerating rules of conduct?
   Have employees been notified that violation of these rules are grounds for disciplinary action up to and including discharge?
   Do these rules of conduct include theft of company, customer, and employee property, including information?
7. Identify off-site locations that should be included in survey, to include warehouses, offices, storage facilities, etc.
   Are these locations protected against vandalism and theft?
8. What is the police agency having jurisdiction over the site?
   Does the plant have dedicated telephone line to this agency?
   Have they been called for assistance in the recent past?
   What has been their response?

Do they normally include any of our perimeter in their patrols?
If requested, would they?

9. Are police emergency numbers readily available to personnel who should have this information?
10. Is information readily available on how to reach the proper agency for assistance with illegal narcotics, bomb threats, obscene calls, etc.?
    Do you have a policy of reporting identifiable items of stolen property to the local police for addition to their files, indexes?
11. Some police agencies have a Crime Prevention Unit that responds to invitations to speak on various topics (drugs, rape, etc.) or that may conduct limited security surveys.
    Is this service available?
    If so, have you taken advantage of it?

Perimeter Security

Lighting Evaluation

12. Is the perimeter adequately lighted?
13. Does lighting aid or inhibit guards in the performance of their duties?
14. Is lighting compatible with closed-circuit television (CCTV)?
    Does it cause monitor to "bloom"?
15. Is the power supply adequately protected?
16. Is lighting properly maintained and cleaned?
17. Are sensitive areas (parking lots, computer areas, stores, storage rooms, shipping/receiving areas) adequately lighted?
18. If an emergency occurred, is the site adequately lighted?
    Is the fenceline adequately lighted?
    In appropriate areas, is glare projection lighting used?

Security Force

19. Proprietary?
    Contract?
    If contract, name of agency and telephone number if proprietary, what is method and source of selection of personnel?
20. Are perimeter patrols conducted? Frequency?
21. Is an incident log, including alarms/responses maintained? Reviewed daily? By Whom?
22. Are security personnel used for nonsecurity related duties?
    If yes, what duties?
23. Does site use photo ID cards?
    Compatible with access control system?
    Who administers it?

24. Are all employees required to show photo ID card upon entry? Is duplicate copy kept on file?
25. Are parking decals or other methods of registering employee vehicles used? Are privately owned vehicles permitted to park on site? If so, can an individual reach a vehicle without passing a guard?
26. Does the site have a receptionist in place at all times? Are visitors required to register? Are they provided with an identifying badge, and are non-company employees escorted while on the site? Is visitor identification verified (e.g., vending company ID, etc.)?

Perimeter Protection

27. If outside building walls form part of the perimeter, are all doors and windows secured against surreptitious entry? Can entry be achieved via the roof? Can hinge pins be removed from doors? Are all entry/egress points controlled when opened?

Internal Security

Lock/Key Control

28. With whom does physical and administrative key control rest?
29. Is a master key system in use?
    How many grandmaster/master keys have been issued?
    Is adequate control exercised over these keys?
30. Is a cross-control system (name versus key number) in use?
    What type of numbering system is in use?
    Is the entire system, including blanks, inventories on a regular basis?
    Are they stamped "Do Not Duplicate"?
31. What level of management authorization (written) is required for issuance of keys?
32. Identify personnel who are permitted to have keys to perimeter fence, doors.
33. Are office/facility keys, particularly masters, permitted to be taken home?
    Are keys signed in/out in a daily log?
34. Are locks rotated?
35. How long has the present lock/key system been in use?
    Have keys been reported lost?
    What level key?
    What is the policy when this happens?
36. Is a record of locations of safes and their combinations maintained?
    Are combinations routinely changed annually and when an individual who knows one no longer has that need to know? (separation, transfer, retirement)
    Are safe combinations, if written, maintained in a secure place?

Alarms and Electronics

37. What type, if any, electronic security system is in use here?
    Do alarms terminate at the site or at an outside central station?
    Has service/response been satisfactory?
38. List alarms such as burglar (doors, windows, space (motion)), duress (receptionist, cashier, nurse), other (card access, CCTV, etc.)

Theft Control Procedures

39. Does the site have a policy of marking items susceptible to theft (calculators, office equipment, hand tools, microwave ovens, TV monitors, VCRs, etc.) so they can be identified as company property?
    Describe the extent of the program.
    Does it include die stamping or etching and painting?
40. Are serial numbers of all items bearing them recorded?
    In the event of theft, is this information related to the police for inclusion in stolen property indexes, and for identification and return in case of subsequent recovery?
41. Are trash receptacles periodically inspected to determine whether items of value may be removed from the site via them?
42. Are all store/office supplies, etc., attended when open?
    What is the procedure for drawing supplies when no attendant is present?
43. Are telephone records properly safeguarded to prevent unauthorized destruction?
    Is access to telephone switching equipment (the “frame room”) restricted?
44. Who performs custodial services—proprietary or contract janitorial people?
    Is access limited to the office area only?
    Are they bonded?
    Are they required to wear ID badges?
    Are they checked during the performance of their duties?
    Are they inspected by guards as they leave?
    Are the janitors’ vehicles inspected on the way off the property?
    How is trash removed from the site?
    Are the vehicles used to remove trash inspected on the way off the property?
    Do the janitors have access to restricted or sensitive areas?
    Are they given office keys (masters?)?
    Are they permitted to take these keys off the site with them?
45. How much cash is kept on site? Is it handled at more than one location?
    How is cash supply replenished?
    Where is it kept during working hours?
    Where is it kept after hours?
    Where are blank payroll checks kept?
    Where are blank disbursement checks kept?

Considering the neighborhood the site is located in, and the amount of cash on site, how do you assess your vulnerability to armed robbery or burglary?

Proprietary/Limited Information

46. Is there Proprietary and/or Limited data on site?
    If so, in what form?
    Is it properly marked?
    Is it stored in a secure location?
    Are the following locked at the end of the day:

    a. Offices?
    b. Filing Cabinets?
    c. Desks?
47. What are office destruction procedures and file purging for Proprietary data?
48. Does the site have a clean desk policy?

Personnel Security

49. Are any background checks conducted prior to employment? Are previous employment dates verified? Are personnel medical records properly safeguarded? Is security included in the new hire orientation? Is company property (credit cards, ID keys) retrieved during exit interviews?

Emergency Procedures

50. Do you have a current bomb threat procedure?
    Who implements it? (searches areas)
    Does the procedure include a checklist for the switchboard operator?
51. Is there a contingency plan for acts of violence?
    A disaster plan?
52. If personnel are required to work alone, are they periodically checked by someone to ascertain their well-being?
    What means do they have of calling for help in an emergency?

Computer Security

53. Are terminated employees immediately separated from the EDP function?
54. Is access to the data center controlled physically, electronically?
    Locked when not in use?
55. Is output distributed via user controlled lock boxes? Is tape library maintained physically separate from machine room?

Threat Information

56. Has liaison been established by your office with the American Embassy Regional Security Officer (RSO)?

Is the RSO able to notify you of security threats concerning known terrorist groups active in the area?
Any groups that harbor hatred for U.S. corporations, your company, its manager, and employees?
Anniversary dates that local population or terrorist groups celebrate?
What tactics and activities are practiced or adopted by local terrorist groups that might affect your company, Its managers and employees?

57. Do you have sources that will inform you of any political controversy or labor disputes that might impact your operations?
58. Will you provide Security with copies of information, that may be detrimental to the company, received as a result of your contracts with the RSO, as well as other sources, including newspaper articles?

APPENDIX II: FACILITY QUESTIONNAIRE

1. Are there any known groups that harbor hatred for U.S. businesses, managers and employees?
   Identify:
2. What terrorist groups are known to be active in the area?
   What tactics have these groups been known to use?
   What is the possibility of a change in these tactics?
3. Are there known groups that vocally oppose foreign capitalism or imperialism in the area?
   Identify:
4. Are there any known groups that vocally or actively oppose the local government that the United States supports?
   Identify:
5. Is there any current political controversy or labor dispute that we should be aware of?
6. Are there any upcoming anniversary dates that the local population or terrorist groups celebrate? Identify:
7. Have there been any previous hostage taking or kidnapping incidents, bombings, assassinations, strikes against U.S. businesses or the government, demonstrations, assaults, sabotage against corporate facilities or products, or occupation of corporate facilities in the area?
   Identify:
8. If there have been previous hostage taking or kidnapping incidents,

   a. How were the victims seized?
   b. What was the fate of the hostages?
   c. How much ransom was demanded?
   d. Was it paid?
   e. How were the negotiations handled?

9. Does the host country prohibit negotiating with hostage takers or prohibit the payment of ransom?
10. Do you consider the local police and intelligence services effective?
11. What are the aims of the local criminals or terrorist groups?
    What tactics or type of activity by these groups would best further those aims?
12. What is the identified groups' capability of carrying out planned activities such as ambush, hostage taking, kidnapping, execution, bombing, etc.?
13. In the event of terrorist activity, which organizations, businesses, groups, or individuals would be the most likely targets?

APPENDIX III: THREATENING PHONE CALL CHECKLIST

PLACE THIS UNDER YOUR TELEPHONE — BOMB THREAT!
QUESTIONS TO ASK:

1. When is bomb going to explode?
2. Where is it right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

EXACT WORDING OF THE THREAT:

Sex of caller:
Race:
Age:
Length of Call:
Number at which call is received:
Time: Date: / /

CALLER'S VOICE:

Calm
Angry
Excited
Slow
Rapid
Soft
Loud
Laughter
Crying
Nasal
Stutter
Lisp
Raspy
Deep
Ragged
Clearing throat
Deep breathing
Cracking voice

Normal
District
Slurred
Disguised
Accent
Familiar

If voice is familiar, who did it sound like?

BACKGROUND SOUNDS:

Voices
Crockery
Clear
Static
Local
Booth
Motor
Factory machinery
Office machinery
Street noises
Animal noises
PA System
Music
House noises
Long distance
Other

THREAT LANGUAGE:

Well spoken
(educated)
Foul
Incoherent
Taped
Irrational
Message read by threat maker

REMARKS:

Report call immediately to:
Phone number
Date / /
Name
Position
Phone number

HOSTAGE!
QUESTIONS TO ASK:

2. Who is this?
3. Where are you calling from?
4. Is this a prank?
5. How do I know this is not a prank?
6. May I talk to the hostage?
7. Is the hostage all right?
8. What do you want?

VERY IMPORTANT:

9. Will you call back in 15 minutes?
10. How can I contact you if I have trouble meeting your demands?

EXACT WORDING OF DEMAND:

Sex of Caller: Race:
Age: Length of call:
Number at which call is received:
Time: Date: / /

APPENDIX IV: LETTER AND PARCEL BOMB RECOGNITION POINTS

WARNING!
LETTER AND PARCEL BOMB RECOGNITION POINTS

- Foreign Mail, Air Mail, and Special Delivery
- Restrictive Markings, such as Confidential, Personal, Etc.
- Excessive Postage
- Hand Written or Poorly Typed Addresses
- Incorrect Titles
- Titles but No Names
- Misspellings of Common Words
- Oily Stains or Discolorations
- No Return Address
- Excessive Weight
- Rigid Envelope
- Lopsided or Uneven Envelope
- Protruding Wires or Tinfoil
- Excessive Securing Material, such as Masking Tape, String, etc.
- Visual Distractions

PERSONAL SECURITY GUIDELINES FOR THE AMERICAN BUSINESS TRAVELER OVERSEAS

Overseas Security Advisory Council

INTRODUCTION

This appendix was developed to inform and make the American business traveler aware of the potentially hostile overseas environment in which they may be traveling or working. The information contained in this appendix will familiarize the traveler with personal security guidelines for traveling overseas. The potential hazards and vulnerabilities that are inherent in protecting/carrying sensitive or proprietary information while traveling are described, as are surveillance and/or targeting recognition, personal conduct abroad, hostage/hijacking survival and fire safety.

There are several scenarios to traveling abroad that are addressed: first, the actual getting from point A to B; second, the airport; third, the hotel or temporary quarters; fourth, traveling within a foreign country; and, lastly, the office or workplace. Each of these five situations presents different potential security problems.

The most effective means of protecting yourself and your property is the liberal use of common sense reinforced with a high state of security awareness. Do not give anyone the opportunity to exploit vulnerabilities. Stay alert and exercise good judgment.

TRAVEL PREPARATION AND PLANNING

Travel Itinerary

DO NOT publicize your travel plans, but limit that knowledge to those who need to know. Leave a full itinerary of your travel schedule, hotel phone numbers and business appointments with your office and with a family member or friend.

Passport

Is it valid? Are the visas current for the country of destination? If not, you and everything in your possession may be looked at in-depth by host government authorities. If you are carrying documents that are sensitive or proprietary, they will be examined in detail to see if there is anything that would be of interest. If there is, you can bet that copies will be made, and there is not much that you will be able to do about it.

Make photocopies of your passport, visa and other important documents that you will be traveling with. Put copies in both your carry on and checked luggage. This makes it easier to replace your identification documents should anything happen. (Also, it is a good idea to leave a photocopy with someone at home.)

Visas

Is a visa required for any of the countries that you are visiting and do you have the appropriate visa(s)? Is the information on your visa application true and correct? In some countries, falsifying information on a visa application can result in an unexpected vacation in the local bastilles.

Some countries are sensitive to which visa you obtain. If you are traveling on business, a business visa should be obtained; otherwise a tourist visa is acceptable.

Medical

Take plenty of any prescription medication with you, as well as an extra set of eyeglasses or contact lenses. Also, take a copy of your prescription should you need to have glasses, contacts or medication replaced. Keep an inoculation record and update it before each trip as each country has different requirements.

- Carry with you a list with your blood type, allergies, medical conditions and special requirements. It is a good idea to have a medical alert bracelet if you have a special medical condition.
- Inoculations—Does the country to be visited require any specific inoculations? This information is available from the embassy or consulate. Be sure to carry your international shot record, just in case.
- If you do not have comprehensive medical coverage, consider enrolling in an international health program. Hospitals in foreign countries do not take credit cards and most will not honor U.S. based medical insurance plans.

Miscellaneous

Keep your personal affairs up to date. If possible, leave a power of attorney with a family member or friend should anything happen to you.

- Do research on the country you will be traveling to before you go. Talk with friends, family or business associates who have visited the country. They can usually give you some good tips for your trip. Also, for any travel warnings or other conditions that you should be aware of, check with the U.S. State Department, Bureau of Consular Affairs.
- Travelers should discuss with their travel agents, which airlines, hotels and car rental companies are recommended.

- Carry in your wallet/pocketbook only the documents you will need. Take only the credit cards you plan to use on your trip.
- If you plan to rent a car, check to see if you must obtain an international drivers permit for the country you plan to visit.
- Obtain information from U.S. Customs regarding any special requirements for the country you are visiting.

Local Import Restrictions

Request from the embassy of the country you plan to visit a copy of any list or pamphlet describing customs restrictions or banned materials. This is a hint designed to minimize the possibility of an encounter with the local authorities.

Leave all expensive and heirloom jewelry at home.

Luggage

DO NOT pack sensitive or proprietary information in your checked luggage. Double envelope the material and hand carry it. Be sure that your luggage is tagged with covered tags that protect your address from open observation. Put your name and address inside each piece of luggage and be sure that all luggage is locked or secured in some fashion.

Luggage Locks

The locks on your luggage are not that secure when it comes to the professional thief or manipulator and are really no more than a deterrent. But, if time is of the essence to the perpetrator, and it usually is when a crime is involved, there are a couple of suggestions that might deter surreptitious entry and/or theft.

- For added security on all luggage, run a strip of nylon filament tape around the suitcase to preclude its opening accidentally if dropped or mistreated by baggage handlers.
- For luggage and briefcases with two combination locks, reset the combination locks from the factory combination (000) to different combinations on each of the right and left locks.
- For luggage with single locks, set the lock on each piece of luggage with a different combination.
- DO NOT pack extra glasses or necessary daily medication in your luggage. Carry it in your briefcase, purse or pocket. If you are the victim of a hijacking you may need these items—if they are in your luggage, you probably will not be able to get to them.
- On your luggage use your business address and telephone number. If possible, use a closed name tag with a cover. Do not use a laminated business card on your luggage, and avoid putting the company name or any logos on your luggage.
- Check with the airline and/or your personal insurance company regarding any lost luggage coverage.

- Make sure you use sturdy luggage. Do not over pack as the luggage could open if dropped. Bind the luggage with strapping so that it will remain intact.
- Never place your valuables (jewelry, money and travelers checks) in your checked luggage. Never leave your bags unattended.
- Consider obtaining a modest amount of foreign currency before you leave your home country. Criminals often watch for and target international travelers purchasing large amounts of foreign currency at airport banks and currency exchange windows.

Airline Security and Seat Selection

- Try to book a non-stop flight, as these have fewer takeoffs and landings.
- Choose an airline with a good safety and on-time record.
- Try to make your stopovers in airports that have a high security standard and good security screening.
- Try to fly wide body planes. Hijackers tend to avoid these as having too many passengers.
- Most travelers prefer an aisle seat. Choose a window or center seat. This will keep you away from the hijackers and any action that may be happening in the aisle.

AT THE AIRPORT

To diminish the risks of becoming an innocent bystander victim of a terrorist attack and reduce your exposure to the criminal threat, there are a number of things that you should remember when checking into an airport.

- In the event of a disturbance of any kind, go in the opposite direction. DO NOT GET INVOLVED!
- Plan to check in early for your flight to avoid long lines at the ticket counter.
- Go directly to the gate or secure area after checking your luggage. (Secure Zone—Area between security/immigration and the departure gate.) Avoid waiting rooms and shopping areas outside the secure areas.
- Stay away from glass wall areas and airport coffee shops which are open to the concourse or public waiting areas.
- From the time you pack your luggage until you check it with the carrier at the airport maintain positive control of all items, both hand carried and checked.
- At many airports security personnel, following FAA protocol, will ask you questions about control of your luggage. Know what items you are carrying and be able to describe any/all electrical items.
- When going through the pre-board screening process cooperate with security personnel and remember that they are there to help ensure that your travel is safe.

- When arriving at or departing from an airport it is a good idea not to be exchanging items between bags while waiting in line for security screening or immigration/customs processing. Complete all packing before entering such areas.
- If a conflict should arise while undergoing the screening process, cooperate. Obtain the names of the screeners involved, and then discuss the matter with a supervisor from the appropriate air carrier.
- Remember that x-ray will not damage film, videos or computer equipment. Many times such items can be cleared using x-ray which means that they will not have to be handled by the screener.
- Consider being transported to/from the airport by a hotel vehicle. Generally the cost is not prohibitive, and arrangements can be made in advance by your travel agent.
- Declare all currency and negotiable instruments as required by law.
- NEVER leave your luggage or briefcase unattended, even while checking in or once in the secure zone. In some countries, the police or security forces assume that an unattended bag is a bomb, and your luggage could be forcefully opened or even destroyed.
- Always be aware of where you are in conjunction with where you are going. If an incident occurs, you need to know how to avoid it and either get out of the area or to your boarding area.
- Dress casually when traveling, as this will keep any undue attention from you. Once aboard the flight, remove your shoes for better circulation. Walk around the flight cabin to keep your blood circulating and swelling down.
- Avoid last minute dashes to the airport.
- Eat moderately, avoid alcoholic beverages and drink plenty of water as this will help to avoid dehydration.
- If possible, before you leave make an effort to adjust your sleep patterns.
- Sleep as much as possible during the flight.
- Carry airsickness medication with you. Even the best traveler sometimes experiences airsickness.
- Avoid a demanding schedule upon arrival. Give yourself a chance to adjust to your surroundings.

SELECTING A SECURE HOTEL

Many U.S. corporations have hotels abroad that are owned by local businessmen and staffed by local workers but managed by first class U.S. hoteliers. You usually can expect levels of safety and security that are consistent with U.S. standards.

- Ask the corporate travel agent for a list of recommended hotels.

- Check with the Regional Security Officer at the U.S. Embassy for a list of hotels utilized by officials visiting the area.

Making Reservations

Make your own reservations when practical and consistent with company policies. The fewer people that become involved in your travel and lodging arrangements, the better.

- If traveling abroad, especially in politically sensitive areas, consider making reservations using your employer's street address, without identifying the company, and using your personal credit card. Again, the less known about your travel itinerary, and whom you represent, the better.
- If arriving after 6:00 P.M., ensure that reservations are guaranteed.
- Request information about parking arrangements if anticipating renting an automobile.
- Be aware that credit card information has been compromised in the past. Always audit monthly credit card statements to ensure that unauthorized use has not been made of your account.
- It is advisable to join frequent travelers' programs available with many lodging companies. These programs enable upgrades to executive or concierge floors where available. Be sure to advise the person taking reservations that you are a member and request an upgrade.

Arriving at or Departing From the Hotel

The most vulnerable part of your journey is traveling between the point of debarkation/embarkation and the hotel. Do not linger or wander unnecessarily in the parking lot, indoor garage or public space around the hotel—be alert for suspicious persons and behavior. Watch for distractions that are intentionally staged to setup a pickpocket, luggage theft or purse snatch.

- Stay with your luggage until it is brought into the lobby, or placed into the taxi or limo.
- Consider using the bellman. Luggage in the "care, custody and control" of the hotel causes the hotel to be liable for your property. Protect claim checks; they are your evidence!
- Keep in mind though that there are limits of liability created by states and countries to protect hoteliers. Personal travel documents, lap tops, jewelry, and other valuables and sensitive documents in excess of $1,000 in value should be hand carried and personally protected.
- If you arrive by auto, park as close to a hotel access point as possible, and park in a lighted area. Remove all property from the car interior and place it in the trunk. Avoid leaving valuables or personal documents in the glove compartment. Prior to leaving the security of the vehicle, note any suspicious persons or behavior.

- If using valet service, leave only the ignition key, and take trunk, house, or office keys with you. Often, valets are not employees of the hotel and work for contract firms.
- Parking garages are difficult to secure. Avoid dimly lit garages that are not patrolled and do not have security telephones or intercoms.
- Female travelers should consider asking for an escort to their vehicles whether parked in the lot or garage.

Registration

In some countries, your passport may be temporarily held by the hotel for review by the police or other authorities, obtain its return at the earliest possible time.

- Be aware of persons in the hotel lobby who may have unusual interest in your arrival.
- If carrying your luggage, keep it within view or touch. One recommendation is to position luggage against your leg during registration but place a briefcase or a purse on the desk or counter in front of you.
- Ground floor rooms, which open to a pool area or beach with sliding glass doors and window access, are considered vulnerable. Depending upon the situation, area, and security coverage, exercise a higher level of security if assigned a first floor room.
- It is suggested that female travelers request rooms that are away from the elevator landing and stairwells. This is to avoid being caught by surprise by persons exiting the elevator with you or hiding in the stairwell.
- Always accept bellman assistance upon check-in. Allow the bellman to open the room, turn lights on, and check the room to ensure that it is vacant and ready for your stay. Before dismissing the bellman, always inspect the door lock, locks on sliding glass doors, optical viewer, privacy latch or chain, guest room safes, dead bolt lock on interconnecting suite door, and telephone. If a discrepancy is found, request a room change.
- Ask where the nearest fire stairwell is located. Make a mental note which direction you must turn and approximately how many steps there are to the closest fire stairwell. In the event of a fire, there is frequently dense smoke and no lighting.
- Also observe where the nearest house telephone is located in case of an emergency. Determine if the telephone is configured in such a manner that anyone can dial a guest room directly, or whether the phone is connected to the switchboard. Most security-conscious hotels require a caller to identify whom they are attempting to telephone rather than providing a room number.
- Note how hotel staff are uniformed and identified. Many “pretext” crimes occur by persons misrepresenting themselves as hotel employees on house telephones to gain access to guest rooms. Avoid permitting a person into the

guest room unless you have confirmed that the person is authorized to enter. This can be verified by using the optical viewer and by calling the front desk.

IN YOUR HOTEL

All hotel rooms abroad are bugged for audio and visual surveillance. This statement, of course, is NOT TRUE, but that is the premise under which you must operate to maintain an adequate level of security awareness while conducting business abroad. Many hotel rooms overseas are under surveillance. In those countries where the intelligence services are very active, if you are a business person working for an American company of interest to the government or government sponsored competitor, everything that you do in that hotel room may be recorded and analyzed for possible vulnerabilities or for any useful information that can be derived from your conversation.

With the basic premise established above, here are some security tips that will minimize the potential risks.

Hotel Room Key

Keep it with you at all times. The two most common ways that thieves and others use to determine if a person is in their hotel room is to look at the hotel room mail slot or key board or call the room on the house phone. If you do not answer the phone that is one thing, but, if your room key is there, you are obviously out and the coast is clear for a thief or anyone else who is interested in searching your room and luggage.

Upon Arrival

Invest in a good map of the city. Mark significant points on a map such as your hotel, embassies and police stations. Study the map and make a mental note of alternative routes to your hotel or local office should your map become lost or stolen.

- Be aware of your surroundings. Look up and down the street before exiting a building.
- Learn how to place a telephone call and how to use the coin telephones. Make sure you always have extra coins for the telephone.
- Avoid jogging or walking in cities you are not familiar with. If you must jog, be aware of the traffic patterns when crossing public streets. (Joggers have been seriously injured by failing to understand local traffic conditions.)

Valuables

Valuables should normally be left at home. The rule of thumb is, if you neither want nor can afford to lose them, DO NOT TAKE THEM! However, if you must carry valuables, the best way to protect them is to secure them in your local offices. If that is not possible, the next best course of action is to seal any valuables by double enveloping, initialing across seams and taping all edges and seams before depositing them in the hotel's safe deposit box or safe.

Luggage

Keep it locked whenever you are out of the room. It will not stop the professional thief or intelligence agent but it will keep the curious maid honest.

Passport

Keep your passport with you at all times. The only time that you should relinquish it is:

- To the hotel if required by law when registering.
- If you are required to identify yourself to local authorities for any reason.

At night, lock your passport and your other valuables in your luggage. This eliminates their mysterious disappearance while you are asleep or in the shower.

Utilize a portable or improvised burglar alarm while asleep. Two ash trays and a water glass are quite effective as an alarm when placed on the floor in front of the entry door into your room. Place a water glass in one ashtray and put the second ashtray on top of the glass. If a straight chair is available, place it next to the door and put the ash tray/water glass alarm on the edge of the chair where it will fall with enough racket to wake you.

GUEST ROOM AS A "SAFE HAVEN"

Hotels are required to provide reasonable care to ensure that guests have a safe and secure stay. Hotels are not required to guarantee guest security. You are responsible for your personal security and property.

- While in the room, keep the door closed and engage the dead bolt and privacy latch or chain. A limited number of hotel emergency keys can override the dead bolt locks. To ensure privacy use the latch or chain!
- Hoteliers provide guest room "safes" for the convenience of guests. However, these containers are not as durable as bank safes and can be breached. Furthermore, the Housekeepers Liability Laws provide that if guest property is not in the "care, custody and control of the hotel," the hotel is not liable. Guests should always place money or valuables in the safe deposit box at the front desk of the hotel.
- When leaving the guest room, ensure that the door properly closes and is secured. Make a mental note of how your property was left; avoid leaving valuables in plain view or in an unorganized manner. A number of hotel employees enter the room each day to clean, repair and restock the room.

Although most hotel employees are honest and hardworking, a few succumb to the temptation of cash or jewelry left unprotected.

- If you determine that an item is missing, conduct a thorough search prior to reporting the incident to hotel security. Do not expect to receive a copy of the security report, as it is an internal document. The incident should be reported to the local police, the Regional Security and Consular Officers at the U.S. Embassy, and your insurance carrier. Hotel security can provide a letter verifying that you reported property missing.
- Prior to traveling, it is recommended that you copy all credit cards, passport, air tickets and other documents to facilitate reporting loss and replacing them. While traveling abroad, secure these documents in the room safe deposit box and carry copies of your passport and visa.
- Request housekeeping make up your room while you are at breakfast, rather than leave a "Please Service This Room" sign on the door knob. This sign is a signal to criminals that the room is unoccupied.
- If you are required to use parking stickers in your auto, be sure that it does not indicate your name or room number.

AROUND THE HOTEL

Most first class international hotels have spent a considerable sum to ensure your safety and security. Fire safety equipment, CCTVs, and security patrols are often part of the hotel's security plan. Regardless of the level of security provided by the hotel, you need to become familiar with certain aspects of the security profile of the hotel. This will take on increased significance when you may be forced to stay at the only hotel at a particular location.

- Vary the time and route by which you leave and return to the hotel. Be alert for persons watching your movements.
- Note if hotel security locks certain access points after dark. Plan to use the main entrance upon return to the property.
- Speak with the bellman, concierge and front desk regarding safe areas around the city in which to jog, dine or sightsee. Ask about local customs and which taxi companies to use or avoid.
- Do not take valuables to the spa or work out room. Note if there are house phones available in the event of a confrontation or emergency.
- Be cautious when entering rest rooms in the hotel. On occasion, unauthorized persons use these facilities to deal drugs or engage in prostitution or theft. Female travelers should be alert to placing purses on hangers on the inside of the lavatory doors, or on the floor in stalls—two frequent locations for grab and run thefts.
- Criminals often use areas around public telephones to stage pickpocket activity or theft. Keep briefcases and purses in view or "in touch" while using phones. Caution is urged in safeguarding telephone credit card numbers.

Criminals wait for callers to announce credit card numbers on public phones and then sell the numbers for unauthorized use.

- Purse snatchers and briefcase thieves are known to work hotel bars and restaurants waiting for unknowing guests to drape these items on chairs or under tables only to discover them missing as they are departing. Keep items in view or "in touch". Be alert to scams involving an unknown person spilling a drink or food on your clothing. An accomplice may be preparing to steal your wallet, briefcase or purse.
- The pool or beach area is a fertile area for thieves to take advantage of guests enjoying recreation. Leave valuables in the hotel. Safeguard your room key and camera. Sign for food and beverages on your room bill rather than carry cash.
- Prostitutes take advantage of travelers around the world through various ploys, use of "knock out" drugs, and theft from the victim's room. Avoid engaging persons who you do not know and refrain from inviting them to your guest room.

FIRE SAFETY FOR THE TRAVELER

Fire safety at home and abroad is a matter of thinking ahead, knowing what to do, and keeping your fear under control. Panic and smoke are the most dangerous threats in the case of a fire. To minimize the risk of a fire, the traveler should remember the precautions listed below and where feasible:

- Stay only at hotels, which have smoke detectors and/or sprinklers installed in all rooms and provide information about fire/safety procedures.
- Request a room between the second and seventh floor. Most fire departments do not have the capability to rescue people above the seventh floor level with external rescue equipment (i.e., ladders).
- Inquire as to how guests are notified if there is an emergency.

Your Hotel Room

- Note the location of the fire exits (stairs) on your floor. Count the number of doors between your room and the exit. If there is a fire, you may have to crawl there in the dark.
- Check exit doors to be sure that they are unlocked and that stairwells are clear of obstructions.
- Note the location of fire alarms, extinguishers and hoses and read any fire safety information available in your room.
- Check outside your room window to ascertain if there is a possible escape route that would be feasible in an extreme emergency.

In Case of a Fire

- KEEP CALM — DO NOT PANIC.
- Call the front desk and notify them of the location of the fire.

- Check your door by placing your palm on the door and then on the doorknob. If either feels hot, DO NOT OPEN THE DOOR.
- If it is safe to exit from your room, head for the stairs. TAKE YOUR ROOM KEY WITH YOU; YOU MAY HAVE TO RETURN TO YOUR ROOM.
- If the corridor is full of smoke, crawl to the exit and again check the doorbefore opening it to see if it is hot. The fire could be in the stairwell.
- DO NOT USE THE ELEVATOR!
- If you can not leave your room or the stairwells are unsafe and you must return to your room:
  - Notify the front desk that you are in your room awaiting rescue.
  - Open a window for fresh air. Do not break the window as you may need to close it again if smoke starts to enter from the outside.
  - Fill the tub and sink with water. Soak towels and blankets as necessary to block vents and openings around doors to keep the smoke and fumes out.
  - Attempt to keep the walls, doors and towels covering vents and cracks cool and wet.
  - A wet towel swung around the room will help clear the room of smoke.
  - Cover your mouth and nose with a wet cloth.
  - Stay low, but alert to any signs of rescue from the street or the halls. Let the firemen know where you are by waving a towel or sheet out the window.

IN THE WORK PLACE

The work place, your home away from home. Here you are safe and secure in the one place where you no longer have to worry about what you do or say. WRONG! You can be just as vulnerable here as anywhere else in the country. You probably are safer, but there are still some precautions that should be taken.

- Safeguard all sensitive or proprietary papers and documents; do not leave them lying around in the office or on top of a desk.
- Guard your conversations so that unauthorized personnel are not able to eavesdrop on discussions pertaining to proprietary information, personnel issues or management planning or problems. In many countries, employees are debriefed by the local intelligence or security services in an effort to learn as much as possible about activities of American companies and their personnel.
- Be careful of all communications. Be aware that the monitoring of telephone, telegraph and international mail is not uncommon in some countries.

TRAVELING BY TRAIN

In many countries, railroads continue to offer a safe, reliable and comfortable means of travel between major metropolitan areas. Other countries, however, operate rail systems that use antiquated equipment, are often over crowded and seldom run on time. As a general rule, the more advanced (socially and economically) a country is, the more modern and reliable will be its rail service. Frequently, rail travel provides a more economical method of travel than other modes of transportation, and frequently it is the only available transportation to smaller cities and towns. However, rail travel can present some security risks to the traveler, just like other means of travel.

Railroads are "soft" targets for several types of criminal or terrorist attacks. They operate over open ground and are easily accessible to the public. The tracks on which the trains operate are in the open for most of the distance they cover. This easy accessibility provides an inviting target for bombings and other forms of sabotage.

The railroad terminals and stations are like self-contained cities, open to the public, frequently for 24 hours a day. They provide a fertile ground for pickpockets, purse snatchers, baggage thieves, bombers and other criminals to operate.

Likewise, trains themselves offer similar opportunities to criminals and terrorists. A train is like a hotel on wheels, offering temporary accommodations, such as restaurants, sleeping space, bars and lounges. All of these can be, and often times are, subject to criminal activities including robbery, thievery, bombing and even, albeit rarely, hostage taking.

Security Risks

Generally, railroad terminals and trains are easy targets for the following types of attacks:

- Bombing and other forms of sabotage to railroad tracks, terminals and trains;
- Robberies and burglaries;
- Theft of unattended baggage on board trains and in rail terminals; and
- Thefts from sleeping compartments.
- Just as air travel calls for planning and preparation to lessen the risks of unfortunate experiences while traveling, rail travel also requires certain preventive measures in order to lessen the likelihood of the traveler becoming a victim. Some of these simple, yet effective, precautions can help make a rail trip a comfortable and convenient means of moving between or within many countries of the world.

Some Precautionary Measures

Prior to Departure:

- It should be noted that many cities have more than one railroad station. Travelers should confirm in advance from which station your train will depart. Make certain that you use the right one.
- Make reservations in advance so that you do not have to stand in the frequently long lines at the rail station ticket counters. This is where pickpockets, baggage thieves and purse-snatchers like to operate. Your

hotel concierge can assist in making your reservations and picking up your ticket.

- Travel light and always keep your luggage under your control. In the time it takes to set down your luggage to check a timetable, a baggage thief can make off with it.
- Watch your tickets. Keep them in an inside pocket or purse to lessen the chance that they can be stolen.
- Do not discard your train ticket until completion of your trip and you have left the arrival area. In some countries you will be required to show your ticket at the exit of the arrival station. If you do not have it, you may be required to purchase another one. Hold on to your ticket, whether or not a conductor checks it.
- Make certain that you board the right car and that it is going to your intended destination.
- Find out in advance if your car will have to be switched to another train en route, when and where this will occur, and the name of the stop just prior to the switching point; be prepared accordingly.
- If you have to transfer to another train to reach your destination, determine this in advance and know where you will make the transfer, the time of transfer, and the train number and departure time of your connecting train (and the track number if possible).
- Learn how to tell if you are in the correct car and if it goes to your destination. Name boards on the side of the car will tell you this.

For example, a name board that appears like this:

VENEZIA

Bologna - Firenze

ROMA

shows that the car began in Venice, stops in Bologna and Florence, and terminates in Rome. Next to the steps leading into the car you should see the numeral "1" or "2," or both. The "1" indicates First Class; the "2" indicates Second Class; and "1" at one end of the car and "2" at the other indicates one part of the car is First Class and the other is Second Class.

- Make certain you know how to spell and pronounce the name of your destination city so you can recognize it when announced.
- Be alert to train splitting. This occurs when part of the train is split off and attached to another train while the remainder of the original train then continues on its way. Check with the ticket agent or on-board conductor to determine this.
- Try not to schedule a late night or early morning arrival. You might find yourself stranded at a rail station with no public transportation.
- Arrange to be met at your arrival point whenever possible.

On Board the Train

- If possible, check unneeded luggage into the baggage car.
- Keep your luggage with you at all times. If you must leave your seat, either take the luggage with you or secure it to your seat or the baggage rack with a strong cable-lock.
- Try to get a window seat. This provides a quick means of escape in the event of an accident.
- Have necessary international documents, including your passport, handy and ready for inspection by immigration officials at each border crossing.
- Always keep your camera and other valuables with you at all times.
- If you have a private compartment, keep the door locked and identify anyone wishing to gain access. Know the names of your porters and ask them to identify themselves whenever entering your compartment.
- When in your compartment, be aware that some train thieves will spray chemicals inside to render the occupant(s) unconscious in order to enter and steal valuables. A locked door will at least keep them out.
- If you become suspicious of anyone, or someone bothers you, notify the conductor or other train personnel.
- If you feel you must leave the train temporarily at a stop other than your destination, make certain that you are not left behind.
- An understanding of military time (the so-called 24-hour clock) will make it easier for you to understand the train schedule.
- Make certain you have currency from each of the countries through which you will be traveling. In some lesser-developed countries (and on some trains) it may be advisable to carry your own food and water.

Upon Arrival

- Make certain that you depart from the train at the correct location.
- Use only authorized taxis for transportation to your hotel or other destination.
- Be alert to criminals such as pickpockets, baggage thieves and/or unauthorized taxi drivers/guides.
- If you do not have a hotel reservation, go to the in-station hotel services and reservations desk for help in obtaining a hotel room.

DRIVING ABROAD

Obtain an International Drivers Permit (IDP). This can be purchased through your AAA Club. Have your passport photos and a completed application. There will be a fee involved. Carry both your IDP and your state driver's license with you at all times.

- Some countries have a minimum and maximum driving age. Check the laws before you drive in any country.

- Always “buckle up.” Some countries have penalties for people who violate this law.
- If you rent a car, always purchase the liability insurance. If you do not, this could lead to financial disaster.
- As many countries have different driving rules, obtain a copy of them before you begin driving in that country.
- If the drivers in the country you are visiting drive on the opposite side of the road than in the U.S., practice driving in a less populated area before attempting to drive during the heavy traffic part of the day.
- Be aware of the countryside you will be driving in. Many countries require you to honk your horn before going around a sharp corner or to flash your lights before passing.
- Find out before you start your journey that has the right of way in a traffic circle.
- Always know the route you will be traveling. Have a copy of a good road map, and chart your course before beginning.
- Do not pick up hitchhikers or strangers.
- When entering your vehicle, be aware of your surroundings.

PERSONAL CONDUCT OVERSEAS

A hostile or even friendly intelligence organization is always on the lookout for sources who are vulnerable to coercion, addictions, greed or emotional manipulation. To eliminate, or at least diminish, the possibility of your doing something inadvertent that would bring your activities to the special attention of one of these agencies, here are some

DO NOT’s to remember:

- DO NOT do anything which might be misconstrued or reflect poorly on your personal judgment, professional demeanor, or embarrassing to you and/or your company.
- DO NOT gossip about character flaws, financial problems, emotional relationships or marital difficulties of anyone working for the company, including yourself. This type of information is eagerly sought after by those who would like to exploit you or another employee.
- DO NOT carry, use or purchase any narcotics, marijuana, or other abused drugs. Some countries have very stringent laws covering the import or use of medications and other substances. If you are using a prescribed medication that contains any narcotic substance or other medication that is subject to abuse, such as amphetamines or tranquilizers, carry a copy of the doctor’s prescription for all medications and check your local restrictions and

requirements prior to departure. Some countries may require additional documentation/certification from your doctor.

- DO NOT let a friendly ambiance and alcohol override your good sense and capacity when it comes to social drinking. In some countries, heavy drinking in the form of toasting is quite common, and very few westerners can keep up with a local national when it comes to drinking the national brew. An intoxicated or hung over business negotiator could, if they are not careful, prove to be very embarrassing to themselves and expensive to the company. In these situations, prudence is essential.
- DO NOT engage in "Black Market" activities such as the illegal exchange of currency, or the purchase of religious icons or other local antiquities.
- DO NOT accept or deliver letters, packages or anything else from anyone unknown to you. You have no way of knowing what you are carrying and it could result in your being arrested for illegally exporting a prohibited item.
- DO NOT engage in any type of political or religious activity, or carry any political or religious tracts or brochures, or publications likely to be offensive in the host country, such as pornography or mercenary/weapons.
- DO NOT photograph anything that appears to be associated with the military or internal security of the country, including airports, ports, or restricted areas such as military installations. If in doubt, DO NOT.
- DO NOT purchase items that are illegal to import such as endangered species or agricultural products.

I'VE BEEN ARRESTED!—WHAT DO I DO NOW?

Foreign police and intelligence agencies detain persons for a myriad of reasons or for no other reason than suspicion or curiosity. The best advice is to exercise good judgement, be professional in your demeanor and remember the suggestions and hints that are listed in this booklet. But, if you are detained or arrested for some reason, here are some points to remember:

- DO ask to contact the nearest embassy or consulate representing your country. As a citizen of another country, you have this right; but that does not mean that your hosts will allow you to exercise that right. If you are refused or just ignored, continue to make the request periodically until they accede and let you contact your embassy or consulate.
- DO stay calm, maintain your dignity and do not do anything to provoke the arresting officer(s).
- DO NOT admit anything or volunteer any information.
- DO NOT sign anything. Often, part of the detention procedure is to ask or tell the detainee to sign a written report. Decline politely until such time as the document is examined by an attorney or an embassy/consulate representative.

- DO NOT accept anyone on face value. When the representative from the embassy or consulate arrives, request some identification before discussing your situation.
- DO NOT fall for the ruse of helping the ones who are detaining you in return for your release. They can be very imaginative in their proposals on how you can be of assistance to them. Do not sell yourself out by agreeing to anything. If they will not take no for an answer, do not make a firm commitment or sign anything. Tell them that you will think it over and let them know. Once out of their hands, contact the affiliate or your embassy for protection and assistance in getting out of the country.

TARGETING RECOGNITION

Any person traveling abroad on business should be aware of the fact that they could be targeted by an intelligence agency, security service or, for that matter, a competitor if they are knowledgeable of, or carrying, sensitive or proprietary information. In the course of doing business abroad, there are certain indicators that may occur which should be recognized as potential hazards and indicative of unwarranted interest in your activities. These situations should be closely scrutinized and avoided if at all possible. A few of the most common scenarios that have been utilized by intelligence/security services and have led to successful targeting and acquisition of information are listed below:

- Repeated contacts with a local or third country national who is not involved in your business interests or the purpose of your visit, but as a result of invitations to social or business functions, appears at each function. This individual's demeanor may indicate more than just a passing interest in you and your business activities.
- A close personal social relationship with a foreign national of a hostile host government is often unavoidable for business reasons. In these instances, be cautious and do not allow the relationship to develop any further than the strictly business level.
- Be suspicious of the accidental encounter with an unknown local national who strikes up a conversation and wants to:
  - Practice English or other language.
  - Talk about your country of origin or your employment.
  - Buy you a drink because they have taken a liking to you.
  - Talk to you about politics.
  - Use a myriad of other excuses to begin a “friendly” relationship.

If any of the above or anything else occurs which just does not ring true, BE SUSPICIOUS!! It may be innocent but, exercise prudence and good judgment.

SURVEILLANCE RECOGNITION

The subject of surveillance is extremely important to anyone conducting business abroad. Surveillance could be indicative of targeting for reasons other than interest by a foreign intelligence or security service. Terrorists and criminals also use surveillance for operational preparation prior to committing other terrorist or criminal acts. It should be noted, however, that the normal business traveler, who only spends a few days in each city and has a low profile, is not really a viable target for terrorists and the risk is very low.

The real terrorist threat to a traveler is that of being at the wrong place at the wrong time and becoming an inadvertent victim of a terrorist act.

Surveillance is an assessment of vulnerabilities in an attempt to determine any information available, from any source, about you or your activities, such as lifestyle or behavior that can be used against you. If the intended target recognizes the fact that he or she is under surveillance, preventive measures can be taken that will hopefully deter further interest. As an example, if the surveillant(s) realizes that he or she has been spotted, then the assumption must be that the operation has been compromised and that the police have been notified or other preventive measures have been taken. On the other hand, if a traveler is being scrutinized by a foreign intelligence or security agency, the surveillance may well continue.

Surveillance takes many forms, from static, such as an observer physically or electronically watching or monitoring your activities in your hotel room or office, to mobile surveillance where the individual being watched is actually followed either on foot or by vehicle.

How do you recognize surveillance? There is only one way: be ALERT to your surroundings. As a traveler, you probably will not be at any one location long enough to know what the norm is in your surroundings, and this puts you at a disadvantage. You will not realize that the person sitting in the car across the street is a stranger and should not be there, whereas a resident would immediately become suspicious.

Be observant and pay attention to your sixth sense. If you get the funny feeling that something is not right or that you are being watched, PAY ATTENTION! That sixth sense is trying to tell you something, and more often than not it will be right.

In any event, report your suspicions or any information to the general manager of the local affiliate or your embassy or consulate just in case something does occur. If there is any question about what actions should be taken, and guidance is not available from the affiliate, contact your embassy or consulate and they will advise you as to what you should do and whether or not the information should be reported to the local authorities. But, the most important thing you should do is making sure that your demeanor is professional and everything you do is above board and not subject to compromise.

If you have reason to believe that you are under surveillance, here is what you should NOT do:

- DO NOT try to slip away or lose the followers as this will probably alert them and belie the fact that you are just a businessperson or tourist going about your business.
- In your hotel room, assume that the room and telephone are being monitored. DO NOT try to play investigator and start looking for electronic listening devices. This again could send the wrong signals to the surveillant. Just make sure that you do not say or do anything in your hotel room that you would not want to see printed on the front page of the *New York Times*.

Response to Targeting

If you have any reason to believe that you are targeted by an intelligence or security service, there is really only one course of action to follow. Report your suspicions to the affiliate or embassy or consulate and follow their guidance.

HOSTAGE SURVIVAL

Any traveler could become a hostage. The odds of that happening are extremely low when the number of travelers is compared to the number of people that have actually become a hostage. However, there is always that slim chance that a traveler could end up being in the wrong place at the wrong time. With this in mind, the traveler should make sure that his/her affairs are in order before they travel abroad. Items of particular importance to an individual in a hostage situation are the currentness of an up-to-date will, insurance policy and a power of attorney for the spouse. If these items have been taken care of before departure, the employee will not have to worry about the family's welfare and the hostage can focus all of his/her efforts on the one thing of paramount importance and that is SURVIVAL!!

To survive, travelers should realize that there are certain dynamics involved in a hijacking or a kidnapping, and, to increase their ability to survive, they must understand how these interacting forces affect the end result. Each individual involved in an incident of this type will have an impact on the eventual outcome. One wrong move by either a victim or a perpetrator could easily result in a disaster rather than a peaceful conclusion to the incident.

The first thing that a traveler should remember is that he or she is not the only one that is scared and nervous. Everyone involved is in the same emotional state, including the perpetrators. Fear can trigger a disaster, and it does not take much for some individuals to set off a defensive spate of violence. Whether it is a demonstration of violence to reinforce a demand or to incite fear in the minds of the hostages, the violence will be motivated by fanaticism and/or fear and that violence will be directed at the person(s) who are perceived to be a threat or a nuisance to the hijackers.

To minimize the possibility of being selected for special attention by the perpetrators and to maximize your ability to survive a hostage situation, here are some guidelines to remember:

Hijacking Survival Guidelines

The physical takeover of the aircraft by the hijackers may be characterized by noise, commotion, and possibly shooting and yelling, or it may be quiet and methodical with little more than an announcement by a crew member. These first few minutes of the hijacking are crucial:

- Stay calm, and encourage others around you to do the same.
- Remember that the hijackers are extremely nervous and are possibly scared.
- Comply with your captor(s) directions.
- If shooting occurs, keep your head down or drop to the floor.
- Remain alert.

Once the takeover of the aircraft has occurred, you may be separated by citizenship, sex, race, etc. Your passport may be confiscated and your carry-on luggage ransacked. The aircraft may be diverted to another country. The hijackers may enter into a negotiation phase, which could last indefinitely, and/or the crew may be forced to fly the aircraft to yet another destination. During this phase passengers may be used as a bargaining tool in negotiations, lives may be threatened, or a number of passengers may be released in exchange for fuel, landing/departure rights, food, etc. This will be the longest phase of the hijacking:

- If you are told to keep your head down or maintain another body position, talk yourself into relaxing into the position; you may need to stay that way for some time.
- Prepare yourself mentally and emotionally for a long ordeal.
- Do not attempt to hide your passport or belongings.
- If addressed by the hijackers, respond in a regulated tone of voice.
- Use your time wisely by observing the characteristics and behavior of the hijackers, mentally attach nicknames to each one and notice their dress, facial features and temperaments.
- If you or a nearby passenger are in need of assistance due to illness or discomfort, solicit the assistance of a crew member first—do not attempt to approach a hijacker unless similar assistance has been rendered by them for other passengers.
- If the hijackers single you out, be responsive but do not volunteer information.

The last phase of the hijacking is resolution, be it by use of a hostage rescue team or resolution through negotiation. In the latter instance, the hijackers may simply surrender to authorities or abandon the aircraft, crew and passengers. In the case of a hostage rescue operation to resolve the hijacking:

- The characteristics of a hostage rescue force introduction into the aircraft will be similar to the hijacker's takeover—noise, chaos, possibly shooting—the rescue force is re-taking control of the aircraft.

- If you hear shots fired inside or outside the aircraft, immediately take a protective position—put your head down or drop to the floor.
- If instructed by a rescue force to move, do so quickly, putting your hands up in the air or behind your head; make no sudden movements.
- If fire or smoke appears, attempt to get emergency exits open, and use the inflatable slides or exit onto the wing.
- Once you are on the tarmac, follow the instructions of the rescue force or local authorities; if neither are there to guide you, move as quickly as possible away from the aircraft and eventually move towards the terminal or control tower area.
- Expect to be treated as a hijacker or co-conspirator by the rescue force; initially you will be treated roughly until it is determined by the rescue force that you are not part of the hijacking team.
- Cooperate with local authorities and members of the U.S. Embassy, Consulate or other U.S. agencies in relating information about the hijacking.
- Onward travel and contact with family members will be arranged by U.S. authorities as soon as possible.

KIDNAPPING SURVIVAL GUIDELINES

Kidnapping can take place in public areas where someone may quietly force you, by gunpoint, into a vehicle. They can also take place at a hotel or residence, again by using a weapon to force your cooperation in leaving the premises and entering a vehicle. The initial phase of kidnapping is a critical one because it provides one of the best opportunities to escape.

- If you are in a public area at the time of abduction, make as much commotion as possible to draw attention to the situation.
- If the abduction takes place at your hotel room, make noise, attempt to arouse the suspicion or concern of hotel employees or of those in neighboring rooms—minimally, the fact that an abduction has taken place will be brought to the attention of authorities and the process of notification and search can begin. Otherwise, it could be hours or days before your absence is reported.
- Once you have been forced into a vehicle, you may be blindfolded, physically attacked (to cause unconsciousness), drugged, or forced to lie face down on the floor of the vehicle. In some instances, hostages have been forced into trunks or specially built compartments for transporting contraband.
- Do not struggle in your confined state; calm yourself mentally, concentrate on surviving.
- Employ your mind by attempting to visualize the route being taken, take note of turns, street noise, smells, etc. Try to keep track of the amount of time spent between points.

- Once you have arrived at your destination, you may be placed in a temporary holding area before being moved again to a more permanent detention site. If you are interrogated:
    - Retain a sense of pride but be cooperative.
    - Divulge only information that cannot be used against you.
    - Do not antagonize your interrogator with obstinate behavior.
    - Concentrate on surviving; if you are to be used as a bargaining tool or to obtain ransom, you will be kept alive.

After reaching what you may presume to be your permanent detention site (you may be moved several more times), quickly settle into the situation:

- Be observant—Notice the details of the room, the sounds of activity in the building and determine the layout of the building by studying what is visible to you. Listen for sounds through walls, windows or out in the streets, and try to distinguish between smells.
- Stay mentally active by memorizing the aforementioned details. Exercise your memory and practice retention.
- Keep track of time. Devise a way to track the day, date and the time, and use it to devise a daily schedule of activities for yourself.
- Know your captors. Memorize their schedule, look for patterns of behavior to be used to your advantage, and identify weaknesses or vulnerabilities.
- Use all of the above information to seek opportunities to escape.
- Remain cooperative. Attempt to establish rapport with your captors or guards. Once a level of communication is achieved, try asking for items that will increase your personal comfort. Make them aware of your needs.
- Stay physically active even if your movement is extremely limited. Use isometric and flexing exercises to keep your muscles toned.
- If you detect the presence of other hostages in the same building, devise ways to communicate.
- DO NOT be uncooperative, antagonistic, or hostile towards your captors. It is a fact that hostages who display this type of behavior are kept captive longer or are singled out for torture or punishment.
- Watch for signs of Stockholm Syndrome, which occurs when the captive, due to the close proximity and the constant pressures involved, begins to relate to, and empathize with, the captors. In some cases, this relationship has resulted in the hostage become empathetic to the point that he/she actively participates in the activities of the group. You should attempt to establish a friendly rapport with your captors, but maintain your personal dignity and do not compromise your integrity.
- If you are able to escape, attempt to get first to a U.S. Embassy or Consulate to seek protection. If you cannot reach either, go to a host government or friendly government entity.

CONCLUSION

It is no wonder that most U.S. business people consider business travel hard work —and one of the most stressful aspects of their job. The running, waiting, and anxiety associated with travel can take its toll on the mind and body. Add an unfamiliar location, a foreign language, and a different culture to the situation and you have the potential for all sorts of problems.

As pointed out in this publication, the keys to safe travel are planning and sound security practices. Proper planning ensures your logistical plan is in place and you have the necessary background information to support your itinerary. Incorporating sound security practices into your travel routine will reduce the likelihood of problems. Together, these keys allow you to get on with the real purpose of your trip.

GLOSSARY

Abridged Security Policy Manual is a simplified manual that tells users what they need to know in order to do their jobs securely. It is important that it be short, relevant, easy to read, but with pointers to the full policies.

Access is the ability to use an information system or enter a physical location.

Access Authority is the person responsible for monitoring and granting access rights to other people.

Access Control is the process of deciding who is given or denied access to an information system or a physical location.

Access Control List is a register of people who have been granted access and the level of access each is allowed.

Actionable Activities are behaviors that create legal liabilities.

Active Competitive Intelligence involves seeking information about strategy, tactics, targets, and technology.

Agroterrorism refers to terrorist attacks on agricultural targets.

American Chemistry Council (**ACC**) is a trade group for the chemical industry that was founded in 1872. It provides information about the industry and campaigns on issues critical to the chemical industry. It created the Responsible Care© program in 1988 to reduce accidents and emissions.

Americans with Disabilities Act (**ADA**) is a federal civil rights law prohibiting the exclusion of people with disabilities from everyday activities, and it includes a requirement that the safety and evacuation special needs of all employees are met.

Antivirus Software scans files for infections. An infection is detected by discovering patterns associated with an infection, which means a program can find only viruses it knows.

Area Challenge involves asking people you do not recognize who they are and why they are in a particular area.

Asset's Vulnerability is determined by the strength of its mitigating controls against the capabilities of a threat.

Attacks on an Organization are crises that involve premeditated actions intended to harm the organization and/or its personnel.

Attack Signature is a sign indicating an attempt at unauthorized access.

Audit Trail records who has accessed an information system and what users did during their access.

Automated External Defibrillator (**AED**) is a computerized medical device. It can check an individual's heart rhythm, recognize a rhythm that requires a shock, and advise the rescuer when it is necessary to deliver an electric shock to a victim of sudden cardiac arrest to restore normal rhythm.

Automated Notification Systems, also known as mass notification systems, are designed to deliver a large volume of text, voice, or data messages to a potentially large audience and in an extremely short amount of time. Normally, the system can send messages through multiple communication channels—not only telephone but also e-mail, pager, fax, instant messenger, PDA, and other channels. To facilitate two-way communication, the notification system should be able to receive an active response, such as a keypad entry, to confirm successful delivery of a message.

Backup is term for copying a file or program.

Badge Challenge involves asking people who they are and why they are in a location if they do not have identification badges.

Baselines, or **Minimum Security Baselines (MSBs),** are operating system specific and provide extensive and minute details of OS configuration settings. The minimum level of assurance that you can have will be your baseline.

Bell-LaPadula Model is an information flow security model. The security clearance and the need to know of each subject and the classification of every object are stored in an authentication database. The security clearance and the need to know of a subject are compared to the classification of the object, if a request for access is initiated. Access is permitted only if the access is in accordance with the stated security policy.

Biba Integrity Model is based on access control rules that ensure data integrity. This model organizes the subjects and objects into groups described by a data integrity level. The subject is restricted from writing to data in a higher data integrity level than its own and cannot be corrupted by data written in a lower level than its own. This model is characterized by the no write up and no read down.

Biometric Information is the electronic storage of physiological and behavioral data. Typical biometric information includes fingerprints, iris recognition, retina recognition, facial recognition, hand geometry, voice recognition, signature verification, and keystroke dynamics.

Biometric Sample is the physiological and behavioral data a user provides to be examined to verify a person's identity and determine access.

Biometric System is an automated system that stores biometric information, compares the stored information, determines whether there is a match, and decides whether the identity has been verified.

Biometric Template is the biometric information about a person that is stored in the biometric system and used as a comparison point to later samples to determine whether or not a person is granted access.

Biometrics use body parts (physiological characteristics) and actions taken by a person (behavioral characteristics) to determine or verify identity.

Black Blocs is the spontaneous collection of anarchists dressed in black.

Brewer and Nash Model provides controls such that there can be no conflict of interest between the subject and the object. A conflict of interest occurs when a trusted subject has competing professional and personal interests. A conflict of interest does not imply that anything improper or unethical has occurred; just that it will be difficult for the subject to make a completely impartial decision. In many cases, third-party verification is required.

Business Continuity can be all the initiatives taken to assure the survival, growth, and resilience of the enterprise.

Business Continuity Plan is an extension of that fundamental business plan that enables a company to achieve its strategic goals under extraordinary conditions.

Business Impact Analysis (BIA) determines systematically how (various) disasters might disrupt processes and what such disruptions would "cost" your business.

Challenges occur when a group accuses the organization of acting improperly or unethically.

Chemical Facility is any plant or warehouse where chemicals are used, manufactured, or stored.

Citizen Corps was created by the Department of Homeland Security and encourages people to take personal responsibility for preparedness by getting trained in first aid and emergency skills and to volunteer to support local emergency management.

Clark-Wilson Integrity Model is designed to formalize information integrity, which is maintained by ensuring unauthorized subjects do not corrupt data in error or with malicious intent. The model defines both certification rules and enforcement rules. Users must use a program to modify the data. This additional layer of protection helps to ensure the integrity of the data. Users are given authorization to use only programs they are allowed to use. The programs permit the user to do only certain things. A third piece of the model revolves around auditing. The model requires the tracking of information that is received from outside the trusted system.

Cloaking refers to efforts to screen an organization's information from the eyes of competitors.

Common Vulnerability Scoring System (CVSS) is an evolving standard for rating software vulnerabilities. The National Infrastructure Advisory Council (NIAC) is responsible for developing the CVSS.

Community Emergency Response Team (CERT) is a program that educates people about emergency preparedness. Community members are trained for hazards that are likely to affect their areas and in basic emergency response skills. Those skills can include first aid, search and rescue, and fire safety.

Competitive Intelligence is the timely, relevant, accurate, and unbiased intelligence on potential threats to an organization's competitive position.

Compromise is when information is given to an unauthorized user or when a security policy is violated, allowing unauthorized or unintentional release of information.

Computer Security Incident is when a security policy or accepted use policy is violated or a violation is attempted.

Controller manages and directs an exercise.

Corporate or Industrial Espionage is the illegal or unethical efforts to collect information for commercial gain rather than national interests.

Corporate Social Responsibility is the management of actions designed to affect an organization's impacts on society. It becomes the actions a company takes to further the social good.

Corruption can be the abuse of commercial position for personal gain. This is called private/private corruption.

Countermeasures are the efforts designed to reduce the vulnerability of an information system or a physical location.

Countersurveillance is a process of collecting and analyzing data. Countersurveillance seeks data on potential attacks.

Criminal History search uses the Social Security number to construct a comprehensive criminal record search. County records are searched for each address connected to the Social Security number along with a search of federal court records.

Crisis is an unpredictable event that poses a significant threat of harm to an organization, industry, or stakeholders if it is handled improperly.

Crisis Command, or **Control Center,** is the physical location where the crisis team meets.

Crisis Management is a set of factors designed to combat crises and to lessen the actual damage inflicted by a crisis.

Crisis Management Plan is a carefully arranged selection of information that can aid a crisis team.

Crisis Management Team is assigned to handle the crisis response and to develop crisis preparation. The team is cross-function, meaning it is comprised of people from different areas of the organization. They meet in a designated area during a crisis and lead the crisis management effort.

Crisis Portfolio/Families are groupings of similar crises used to develop a set of crisis management plans.

Crisis Sensing is the process of identifying and disarming potential crises.

Crisis Sensing Mechanism is a systematic approach to collecting and analyzing prodromal information/crisis warning signs.

Crisis Spokespersons are the organization representatives that speak for the organization during a crisis. Their primary role is to speak with the news media.

Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary partnership between the private and public sectors intended to reduce the threat of terrorism while also facilitating the speed of international trade.

Cyberslacking is when employees use the Internet, including e-mail, for personal use and waste time while at work.

Data Mirroring refers to the real-time backup of data.

Decryption is the process of converting ciphertext to plaintext.

Defamation is a false statement that hurts someone's character or good name.

Defensive Competitive Intelligence is preventing competitors from collecting information about your organization. It tries to make it more difficult for competitors to find useful information about your company.

Dictionary Attacks are attempts to break password protect by simply guessing words from the dictionary.

Digital Signature provides verification that an e-mail is really from the person claiming to have sent it and that the e-mail has not been altered.

Digital Video Surveillance is networked IP-based. The video surveillance is a component of the IT network. Each camera has an IP address and is controlled centrally through a software application. The video surveillance transition to digital is another illustration of the convergence of physical and IT security.

Distributive Justice involves perceptions with the fairness of outcomes. Employees determine whether the effort they put into their jobs results in equal rewards from their jobs.

Document Management System tracks a document's versioning/history, maintaining a record of revisions that could prove crucial if verifying when a specific requirement of a policy took effect were to become necessary. It also helps with archiving, retention, distribution, and work flow.

Drill is a supervised, coordinated activity used to test a specific operation of part of a response plan. The idea is to work on smaller parts of the response plan before integrating these components into a large drill that tests them all.

Drug Screening or **Testing** uses samples of urine, oral fluid, or hair to determine whether a person has used certain substances.

Drug Tests are processes used to detect the presence of drugs.

Due Care is the care that a reasonable person or company would exercise to secure its data, physical security, or other protective actions in an organization.

Due Diligence determines whether due care has actually occurred.

Dumpster Diving involves digging through trash for information.

Ecodefense are strategies to defend the environment.

Ecoterrorism involves attacks by environmental groups on individuals or property.

Education Verification verifies all degrees claimed by the applicant. The information obtained includes the name of the institution, date of graduation, dates of attendance, degree obtained, and type or field of study. Applicants who are currently students can be checked for degree progress, field of study, and planned graduation date.

Emergency is any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public reputation.

Emergency Operations Center is a base of operations for those charged with managing emergencies, directing emergency response teams, assessing and controlling physical damage, coordinating with public safety officials, and providing status reports to management.

Emergency Planning & Community Right-to-Know Act (**EPCRA**) is part of Title III of the 1986 Superfund Amendments and Reauthorization Act (SARA). EPCRA seeks to identify the amounts of chemicals located at, or released from, facilities; to understand the potential problems that hazardous materials pose to the surrounding communities and environment; and to provide information to the public/local community and the local emergency planning and response organizations. EPCRA has four sections that cover emergency planning, emergency notification, community right-to-know hazardous chemical reporting, and community right-to-know toxic chemical release inventory reporting.

Emergency Preparedness and Response centers on a plan of action to commence during or immediately after a disaster to prevent loss of life and minimize injury and property damage. It includes developing emergency response procedures and establishing training for all employees on the proper actions to take in response to emergency and disaster situations and training for employee emergency response teams (emergency response teams, fire safety teams) on their roles and responsibilities. Also included is the acquisition and maintenance of life safety systems and emergency supplies and equipment.

Emergency Response Teams (**ERTs**) are the people responsible for executing an organization's emergency response and preparing for that response. The team receives training on the overall emergency management program and its specific roles and responsibilities.

Employee Background Check or **Investigation** is an inquiry into a person's character, personal characteristics, or general reputation.

Employee Special Needs Form is a means of identifying employees with special needs in emergency situations. The forms are distributed and employees are invited, not required, to complete and return the form.

Employer Reference Check verifies past employment by checking with the human resource departments of previous employers. The search can check dates of employment and job titles. Applicants must grant approval for this contact.

Encryption is a coded message, an excellent choice for sensitive information. Unless the person has the key for decoding the message, all that will be seen is a random series of characters, letters, and numbers. It is a process of converting plaintext into ciphertext using an encryption program.

End-to-End Encryption involves the process of encrypting a message and sending it through a system.

Ethical Conduct Audit is a systematic measurement of the people, perceptions, behaviors, decisions, and processes in the context of their work activities using a reliable and valid method to discern with greater certainty the status of ethics and compliance within the company.

Ethical Misconduct Disasters (EMDs) are specific, unexpected, and nonroutine unethical events or a series of unethical events that creates significant operational disruptions and threatens, or is perceived to threaten, an organization's continuity of operations.

Ethics and Compliance Programs cover behaviors related to compromising the following: customer or marketplace trust, shareholder or organizational trust, employee trust, supplier trust, and public or community trust.

E-vaulting is a general term describing a number of different data backup methods.

Exercise is a focused practice activity that puts organizational personnel into a simulated situation requiring them to act as they are expected to in a real event.

Expected Actions are the actions or choices that you want players in an exercise to carry out in order to demonstrate their competence. In short, it is what you want people to do so you can evaluate their proficiency.

Facilitation Bribes (Grease) are small amounts of money that speed up legitimate transactions.

False Acceptance is when a biometric system wrongly identifies a person or incorrectly verifies an impostor.

False Acceptance Rate is the probability that a biometric system will make an error by incorrectly identifying a user or allowing entry to an impostor.

False Positive is created when a person asks a question that when answered provides a sense of comfort that does not reflect the actual state of affairs.

False Rejection is when a biometric system does not identify an applicant or fails to verify a true user.

False Rejection Rate is the probability that a biometric system fails to properly identify a legitimate user of a system.

Financial Risk is comprised of multiple areas of risk such as credit risk, interest rate risk, and market risk, to name just a few.

Firewalls can be hardware or software designed to protect your computer from attackers.

Food Safety Inspection Service (FSIS) has resources to help small and very small companies address food security issues. The FSIS provides model plans for a variety of food industry establishments that can be adapted to fit the security and budgetary needs of a company.

Food Security guards against intentional acts of contamination or tampering.

Foreign Corrupt Practices Act requires any publicly traded company to maintain accurate records of all transactions and to have an adequate set of internal accounting controls. The act is designed to prevent corruption by making it difficult to hide money used for bribes.

Full-Scale Exercise simulates an actual event as closely as possible. Equipment is used, people mobilized, and simulated victims appear. The organization often coordinates the full-scale exercise with local emergency responders. These responders get practice, and the organization better understands how to coordinate responses with these units. Your people are on the scene moving and using equipment as they would in the actual event, as well as coping with the simulated victims.

Functional Exercise tests the capabilities of the organization to respond to a simulated event. As a simulation, it is interactive and time pressured. Events and information unfold in real time. The functional exercise allows an organization to examine the coordination, interaction, and integration of its roles, policies, procedures, and responsibilities.

Functions in exercises are actions or operations required during a response.

General Crisis Management Skills are knowledge, skills, and traits that are unique to a crisis management team. The two key skills are decision making and listening.

Graham-Denning Model addresses those issues involving granting rights to users and how the users can use those rights on objects. The model uses eight basic protections.

Guidelines are written to the same level of technical detail that standards are. The difference is that guidelines are sets of procedures that are suggestions, not mandates.

Hazard is the technical or scientific assessment of risk based on likelihood and impact.

Hazard Vulnerability assesses the factors that can cause the most damage to your facility and your operations.

Hidden Mode prevents other users from discovering your wireless connection. Only paired devices can find one another in this mode.

Hot Site is the term used in business continuity to indicate a facility that is fully operational and can be used if an existing facility is damaged or cannot be accessed for some reason.

Inappropriate Usage is when someone violates accepted computing practices.

Incident is a violation or threat of a violation of information security policies or accepted use policies.

Indirect Bribe is when an organization pays some agent or intermediary who helps negotiate a deal and employs bribes as part of its negotiations.

Information Security (**Cyber Security**) describes efforts to prevent, detect, and respond to attacks on a company's information with a focus on computer systems.

Information Security Awareness is a communication effort designed to make users aware of information security concerns and the need to address them.

Information Security Awareness and Training Program is a communication program designed to teach users about information security policies and procedures.

Information System is a defined set of information resources that serves to collect, process, maintain, use, share, and disseminate information.

Insider Threat is when employees, contract workers, or former employees use their knowledge of an organization's information system to violate information security.

Instant Background Check is a computer search of a rather limited database. Such checks are fast but not very accurate.

Integrity represents efforts that seek to protect information from improper modification or destruction.

Integrity Management includes creating formal and informal systems to ensure that employees will act in ways that are legally compliant as well as enact the corporate code of conduct goals in consistently professional, ethical, and desirable ways. Integrity management is intertwined with managing the larger corporate culture and informal reward/motivation processes that impact employee decisions and behaviors in ways that transcend policies printed in a written code of conduct.

Interactional Justice involves perceptions of the quality of interpersonal treatment during procedural justice episodes. Did the people in charge of the procedural justice treat those involved with dignity and respect?

Intrusion Detection System is software that scans for suspicious activity and warns the administrator of these actions.

Intrusion Prevention System is a system that detects an intrusion and takes actions to prevent it.

Issues Management is a systematic approach intended to shape how an issue, a type of problem whose resolution can impact the organization, develops and is resolved.

Key Exchange is when people exchange public keys so that they can exchange secure messages.

Key Pair is a set of keys that allows a message to be encrypted and then decrypted using the other key. The pair is usually a public key and its matching private key.

Keys are used to create a digital signature and each signature has two keys, a private key and a public key. A private key is used by the person sending the e-mail message and is password protected. A public key is made available to the receiver of the message and is used to verify the signature.

Learnable Risk is one that management can make less uncertain if it can commit the time and resources to learn more about it.

Least Privilege Principle is when each employee is given only the minimum access required to complete his or her job.

Legal Risks are the uncertainties resulting from legal actions or ambiguity in the applicability or interpretation of laws, contracts, or regulations.

Libel is written defamation.

Logic Bomb is a form of malicious code that is embedded in a system and timed to activate at a later date.

Low-Hanging Fruit is the easiest target for social engineers.

Management Misconduct is when management has intentionally placed stakeholders at risk or violated legal or regulatory statues.

Military Record Verification contacts military branches to verify dates served and type of discharge.

Mitigation involves actions taken to eliminate or reduce a hazard and the risk it poses to an organization.

Monkeywrenching involves violent forms of ecodefense including arson, tree spiking, billboard vandalism, road reclamation, and ecotage (eco-sabotage).

Motor Vehicle Records Check provides information on an applicant's driving history. The data would include speeding or moving violations, chargeable accidents, DUIs/DWIs, suspensions or revocations, and accumulation of points.

Multilevel Security Policy is one in which the computer or database contains information that has different security classifications (top secret, secret, confidential, unclassified).

Muster Area is a designated area where people are to gather during emergencies.

Narrative briefly describes the events that occurred right before the exercise began. The narrative sets the mood for the exercise as well as the stage for later actions by providing the initial information players use to make choices and take actions.

Negligent Hiring occurs when a company fails to screen employees properly and the hiring results in injuries.

Negligent Retention occurs when a company keeps an employee on staff after learning this employee is unsuitable and injuries occur.

Negligent Supervision involves a failure to provide the proper oversight to ensure that employees perform their jobs properly.

Noncompete Agreements are part of an employment contract or separate agreements that prohibit an employee from working in the same business for a specified length of time. The idea is to prevent employees from using a company's confidential information against it.

Nondisclosure Agreements (NDAs) are contracts that require parties to protect the confidentiality of secret information that they learn during employment or through some other business transaction.

Noninterference Model states that transactions at one level of a system will not affect the state of the system at a lower level of the system. If a transaction that has occurred at a level above me changes my state of the system, then I might be able to deduce what that transaction was.

Non-Repudiation is the guarantee that the information sent has been delivered and the receiver has proof of the sender's identity.

Object is the thing that is requested in an information system.

Operational Risks include a shortage in the workforce or equipment breakdown or other events that may impact businesses.

Organizational Culture is the way things are done in an organization. It represents the beliefs, values, norms, and practices that are taken for granted in an organization and guide actions in the organization.

Orientation Session introduces the plan and process. The purpose is to familiarize people with their roles, plans, procedures, and equipment. It can also help them understand how to coordinate activities and clarify their responsibilities.

Outrage is the emotional and subjective reaction to risk.

Outrage Management is a type of risk communication intended to help people to understand that a risk is not as bad as they think it is.

Outside Threat refers to unauthorized entry by a person who is not a member of a secure domain.

Outsourcing is when management shifts noncore operations from internal production to an external entity that specializes in that operation.

Packet Sniffer is software that records and watches network traffic.

Pandemic is a global disease outbreak.

Passive RFID Tags have no power source and are read by scanners from short range.

Passwords limit computers to authorized users. They are one form of authentication. Strong passwords include a combination of letters (upper and lower case), special characters, and numbers.

Patches are updates to software programs that prevent the exploitation of known vulnerabilities. Using patches reduces the risk of attackers inflicting harm by exploiting the vulnerability.

Personal Identification Number, or **PIN,** is a password composed of decimal digits only.

Petty Corruption involves small amounts of money.

Phishing Attacks purport to originate from a financial institution and ask (though sometimes warn) users to update their personal account information by clicking on the attached link and providing what is required.

Physical Security includes efforts to monitor and control the facility's exterior perimeter and interior space.

Piggyback is a way of getting around swipe cards. When a legitimate person is entering, another person claims to be late for a meeting and says he or she left his or her badge on the desk or offers some other excuse. The person then gains entry without a valid swipe card.

Policies are guiding principles that establish management's authority and responsibility to create a secure business environment, outline acceptable and unacceptable behaviors and activities, and present specific direction toward the basic goal of protecting the organization's people, facilities, physical assets, and information assets. A policy is a formal statement of rules that people who are given access to an organization's technology and information assets must follow.

Political Risks include changes in leadership, civil unrest, and war or other political events that may have an impact on a company's ability to operate.

Precaution Advocacy is a type of risk communication designed to get people to be concerned and to take the risk seriously when people are not concerned enough about a risk.

Preemployment Evaluation Report Credit Report, or **PEER,** uses the national credit bureau database to provide the applicant's national credit history. The report will reveal any bankruptcies, tax liens, foreclosures, or repossessions.

Prime Movers are powerful figures in the organization that others look to for guidance or rely on as important sources of information.

Principle of Separation of Duties states that each transaction is divided into a number of smaller transactions. These transactions are then assigned to separate individuals to accomplish.

Procedural Justice involves perceptions of the fairness of procedures. Are procedures implemented consistently, without bias, and do they consider the interests of all parties and provide a means for correcting errors?

Procedures are documents that provide the step-by-step instructions necessary to reach a desired end state. They are specific operational steps that individuals must take to achieve goals that are often stated in policies.

Processes are activities, tasks, and procedures typically performed across multiple organizations to implement company policies and standards.

Prodromes is a name used to refer to the warning signs of a crisis.

Product Harm is when a product that an organization makes can hurt consumers in some way.

Product Tampering is when an individual or group alters a product to cause harm or for its own financial gain.

Professional License Verification verifies an applicant's professional license or certificate through the accrediting agency or professional association. This information includes the license number, expiration date, type of license or certificate issued, date of issue, and whether there have been any disciplinary actions or sanctions against the license or certificate holder.

Propaganda of Deed uses direct actions against organizations to inspire revolution or change.

***-Property** (**read star-property**). This is the no write-down rule. It states that a subject with a secret classification cannot write into a document with a classification of confidential or unclassified.

Public Key is the half of the key that is available to verify signatures or encrypted information.

Purpose Statement is a broad articulation of the exercise goal that guides the entire exercise. The purpose statement limits the objectives and clarifies to participants why the exercise is being conducted.

Radio Frequency Identity (**RFID**) is a system of technology components used to track "things." Its primary use is to follow the movement of items through the supply chain. As such it can be an important component in supply chain security. The central component of the RFID is a wireless radio frequency device known as a tag.

Random Risks are such that no amount of analysis of causes or drivers can make them less uncertain.

Recovery Planning involves making provisions for first aid, search and rescue, building evacuation, and emergency communications; coping with fires and hazardous materials; and general personnel training in all of the above.

Remote Access is when a user accesses an information system from outside of the security parameters of the information system.

Remote Video Auditing (**RVA**) is the use of digital cameras to observe specific employee behaviors such as customer service or areas that involve regulatory compliance activities. The video is reviewed and critiqued by auditors.

Reputation (of an organization) is an aggregate evaluation stakeholders make about how well an organization is meeting stakeholder expectations based on its past behaviors. In other words, a reputation is an evaluation of an organization based on stakeholder perceptions of an organization.

Rescreening of Employees typically involves drug testing, random or follow-up, and periodic background rechecks.

Residual Risk is the potential risk that exists after efforts have been taken to reduce the risk.

Resume Fraud is when job applicants place false information on their resumes.

Risk is the likelihood that something bad is going to happen and the associated impact.

Risk Analysis is a formal review of the risks in a system that involves assessing the likelihood of the risk, the impact of the risk, and efforts to mitigate the risk.

Risk Assessment is the process of evaluating the likelihood that a negative event is going to occur and the estimated magnitude of loss.

Risk Bearers are people who must live with the possible consequences of a risk, such as those living near a chemical facility.

Risk Communication is a conversation about risk between an organization and its stakeholders, typically the community members living near a facility. The focus of risk communication is helping people to understand/evaluate the risk and to manage it.

Risk Management is the process of identifying, assessing, and addressing the risk.

Risk Tolerance is the amount of risk an organization can accept in efforts to achieve its objectives.

Rumors are untrue information about your organization that is publicly circulating.

Scope sets limits to an exercise.

Secure State Machine Model is when you can show that after every possible state transition action, the machine ends up in a secure state.

Security Architecture is the framework of the organization's security system.

Security Documentation defines the scope of security in the organization and determines what is to be protected and the extent of that protection. It also explains what is expected from employees and what the consequences are of noncompliance.

Security Model is a scheme or framework for specifying and enforcing the organization's security policies.

Sensitive Information includes mission critical data, private customer information, private employee information, proprietary information, data used to calculate the organization's financial performance, and any information that would damage an organization if it were to be exposed.

Shelter-in-Place means that people should stay inside of buildings and seal the buildings off from outside air.

Shoulder Surfing is simply watching as the employee logs in and then exploiting the network from home later.

Silo Effect is when business units seem to operate almost autonomously with little understanding of what other departments are doing and how they impact one another.

Silos are self-contained departments or other business units that struggle when communicating or working with other departments or silos.

Simple Security Property states that subjects cannot read up. Subjects cannot read an object with a higher classification than their security clearance.

Simulators in exercises provide messages to participants in a carefully planned sequence that mimics the actual event.

Slander is spoken defamation.

Smishing uses a text message sent to cell phone users, usually informing them that they have enrolled in a service of some sort and will be charged unless they visit a listed web site to unsubscribe. Visiting the site loads malware on the victim's computer.

Social Engineers are individuals who use charm, guile, and wit to secure information—or perhaps even direct system access—in order to achieve their goals.

Social Security Number Trace determines whether the Social Security number belongs to someone who is dead and lists all the names and addresses associated with that Social Security number.

Spear Phishing involves sending the fraudulent e-mail only to customers of the institution in question, in contrast to a standard phish e-mail that is sent to as many e-mail addresses as the scammer can find.

Spyware, or **Adware,** is used by advertisers to control material people see when they are online. Spyware can send you pop-ups, redirect your browser to a web site, or track your Internet activities.

Stakeholder Churn is when stakeholders are angry at an organization. Angry stakeholders can make it harder for an organization to operate.

Stakeholders are any group that can affect or be affected by the behavior of an organization. Common stakeholders include customers, suppliers, investors and financial analysts, community members, employees, the news media, government agents, and activist groups.

Standards are more issue specific than policies, usually focus on one technology, and have a shorter life span. They are sets of rules for implementing policy.

State Transition Actions are those processes that will alter the state of the information system.

Strategic Partnership Program Agroterrorism (**SPPA**) is a collaborative initiative designed to protect the food supply of the United States. The collaboration includes the Department of Homeland Security (DHS), U.S. Department of Agriculture (USDA), Food and Drug Administration (FDA), and Federal Bureau of Investigation (FBI), along with private industry, trade associations, and the states.

Subjects are any entities that request access in an information system.

Supply Chain is the series of steps from the extraction of raw materials to the finished product. These connections require a coordinated system of organizations, people, activities, information, and resources to move a product or service from supplier to customer. Every organization that comes into contact with a product is part of its supply chain.

Suspected Terrorist Watch List Search determines whether the applicant is on a suspected terrorist watch list.

Tabletop Exercises are designed to be low-stress analyses of problematic situations an organization is likely to face. The tabletop, led by a facilitator, is not an attempt to simulate the event or use equipment, but is just an analysis of the situation. Participants improve their critical thinking skills by analyzing and resolving problems using plans and procedures. The key is to have participants identify and analyze the problem areas.

Tags are small devices for RFID that have a transponder and an antenna. The tags transmit data signals when powered/queried by an RFID on the tag's frequency.

Technical Error Industrial Accidents refer to situations in which the cause is beyond the reasonable control of a person or the organization.

Template is the biometric data stored by a system and used for comparison purposes for verification.

Terrorism involves the unlawful use of force and violence against people or property that is intended to intimidate or coerce some group.

Threat is anything that can have a harmful effect on an organization.

Ticketing System is a procedure that shows who is responsible for an action, such as correcting the vulnerabilities, and the deadlines for the responsible person to take the action.

Transparency is a principle that seeks to make the operations of an organization visible to stakeholders. It typically involves the reporting of facts and figures along with the process that organizations use to make decisions.

Trojan Horses are software that pretends to be something else. They claim to do one thing but perform other nefarious operations in the background.

Trusted Subject is one that has proven to be trustworthy. Trustworthy means that subjects always manually perform functions within the security policy. Trusted subjects can transfer information from a higher-classified object to a lower-classified object.

Unauthorized Access is when a person gets into an information system without permission or when users access information they are not supposed to access.

Unauthorized Disclosure occurs when unauthorized people are given access to information.

U.S. Chemical Safety Board is an independent federal agency that is responsible for investigating chemical accidents. The focus of its work is on identifying the root cause of chemical accidents at fixed industrial facilities.

U.S. Customs and Border Protection (**CBP**) is part of the United States Department of Homeland Security. Its actions cover enforcing U.S. trade law, regulating and facilitating international trade, and collecting import duties. The CBP also has responsibilities for preventing terrorists from entering the United States, preventing illegal drugs from entering the United States, and protecting American businesses from the theft of intellectual property.

USDA's Agriculture Marketing Service (AMS) works with the Cotton, Dairy, Fruit and Vegetable, Livestock and Seed, Poultry, and Tobacco commodity programs. AMS provide standardization, grading, and marketing news for these six commodities. AMS also enforces federal laws including the Perishable Agricultural Commodities Act and the Federal Seed Act.

United States Department of Homeland Security was created by the National Strategy for Homeland Security and the Homeland Security Act of 2002. Its goal is to create a large network with a unified core that seeks to improve the security of the United States.

User is a person who has authorized access to an information system.

User Registration is when a person is granted access to a secure domain.

Vendor Vulnerability Identification and Control refers to establishing minimum acceptable criteria for vendor vulnerability identification and control methodologies, as these methodologies relate to vendor business continuity programs and plans, and the ability of the vendor to integrate its methodologies on a sustainable basis with the client's business continuity management strategy.

Verification is a process that determines whether the claimed identity is correct. The process involves comparing the claim to some stored information for the user.

Video Surveillance Policy lets employees know where and how they will be observed by video cameras.

Virtual Teams are when not all team members are in the same physical space with face-to-face contact. Various communication technologies are used to connect the members to the team.

Viruses are the codes we hear the most about in the news. To get a virus, you must actually do something that allows the code to infect your computer, such as open an infected file.

Vishing leverages voice-over IP (VoIP) technology to dial victims with a message that their credit card has had recent fraudulent activity. The victim is asked to type in his or her credit card information.

Vulnerability is a weakness that could be exploited or create a harmful event such as a crisis or security breach.

Vulnerability Assessment is a formal analysis and evaluation of vulnerabilities in an organization.

Vulnerability Discovery involves the procurement, placement, and scheduling of a vulnerability scanning tool.

Warm Site is term used in business continuity to refer to a facility that is partially equipped and can be used to cover some functions when there is a significant business disruption.

Workers' Compensation Record Search is a search of an applicant's accident dates and nature or type of injuries involved. Such searches can be done only in states that permit the dissemination of workers' compensation claim history and must be used in compliance with the Americans with Disabilities Act guidelines. The State Workers' Compensation Commission of the Industrial Relations Board will provide this data.

Workplace Aggression consists of efforts by current or past employees to harm current employees or the organization.

Workplace Aggression Tolerance Questionnaire (**WATQ**) is a twenty-eight-item instrument used to assess how willing people are to accept a variety of workplace aggression behaviors.

Workplace Violence involves someone in the workplace becoming a victim of a violent act. The violence may be perpetrated by a random customer, another employee, a former employee, or by someone else the person knows, such as an enraged spouse.

Worms are malicious programs that can move through systems without any help from a user. The worm uses weaknesses in software to infect a computer. Worms can also be spread via e-mail and web sites but are self-propagating.

INDEX

ABOUT THE EDITOR AND CONTRIBUTORS

W. TIMOTHY COOMBS, Ph.D., is an associate professor in the Department of Communication Studies at Eastern Illinois University. He is the 2002 recipient of the Jackson, Jackson and Wagner Behavioral Science Prize from the Public Relations Society of American for his crisis research. His research has led to the development and testing of the Situational Crisis Communication Theory (SCCT). He has published nationally and internationally in the areas of crisis management and preparedness. His works have been translated into Chinese, Dutch, and German. Dr. Coombs, who received his Ph.D. from Purdue University, has published twenty-five professional articles, over thirty academic journal articles, and thirty book chapters. He has also published two coauthored books and two of which he is the sole author, including the award-winning *Ongoing Crisis Communication* (now in its second edition) and *Code Red in the Boardroom: Crisis Management as Organizational DNA* (Praeger, 2006). He was part of a forum at the Batten Institute at the Darden School of Management, "Defining Leadership: A Forum to Discuss Crisis Leadership Competency" and has a chapter in the related *Executive Briefing on Crisis Leadership.* Dr. Coombs has lectured at various venues in the United States, Europe, and Australia on the subject of crisis management and related topics. He has also consulted with companies in the construction, airlines, petrochemical, and health care industries on crisis-related topics. Dr. Coombs does consulting work through Communications Northwest, LLC.

ROBERT C. CHANDLER, Ph.D., is professor and chair of communication in the Communication Division at the Center for Communication and Business at Pepperdine University. Dr. Chandler is a member of numerous academic associations including the National Communication Association, International Communication Association, Western States Communication Association, American Forensics Association, and the American Academy of Experts in Traumatic Stress. He is an expert in organizational and business communication; crisis communication; communication during emergencies, crises, and disasters; communication priorities for pandemics and other public health crises; risk communication; behavioral and psychometric assessment and appraisal; leadership; multicultural diversity; organizational integrity; employee ethical conduct;

and business ethics. He is an acclaimed speaker, presenter, and trainer in a wide range of organizational and corporate settings including national Webinars, DRJ World Conference, Contingency Planning and Management, Continuity Insights Management Conference, RSA Conference, and the International Security Conference. Dr. Chandler is an accomplished researcher and scholar with more than one hundred academic and professional papers, including widely circulated white papers on communication during disasters. The author of more than fifty publications, he is the author or coauthor of several books including *Crisis Communication Planning; Terrorism: How Can Business Continuity Cope?; Disaster Recovery and the News Media;* and *Managing the Risks for Corporate Integrity: How to Survive an Ethical Misconduct Disaster*.

DOUGLAS G. CONORICH is the global solutions manager for IBM Global Services' Managed Security Services (MSS). In this capacity, he has responsibility for developing new security offerings, ensuring that the current offerings are standardized globally. He oversees all training of new members of the MSS team worldwide in how to do "ethical hacking" and service delivery. Mr. Conorich has over thirty years' experience with computer security, holding a variety of technical and management positions. He has expertise in the areas of systems security management, including security policy generation and review, security implementation, audit verification procedures, encryption management, and security product design. Mr. Conorich is a networking and UNIX expert, with more than fifteen years' experience in these areas. He has undergraduate degrees in physics, computer science, and meteorology and a master's degree in physics from the University of New Mexico.

ÁGNES HUFF, Ph.D., is president and CEO of Ágnes Huff Communications Group, LLC. She has over twenty years' experience in public relations, marketing communications, crisis management, and strategic counseling. In 1995, she founded Ágnes Huff Communications Group, LLC, a full-service marketing communications firm located in Los Angeles, specializing in integrated communications. The firm is a certified MBE/SBE with the state of California and the county and city of Los Angeles. Through her relationships with the media, Ms. Huff's clients have appeared on the covers of *Fortune* and *CFO Magazine* and have been prominently featured in *Forbes*, the *L.A. Times*, *USA TODAY*, and the *Wall Street Journal*, as well as on ABC, CBS, CNN, and E! Entertainment. With her background in psychology, Ms. Huff brings a depth of understanding and dimension to her work that is generally not found in a traditional agency setting. With crisis management as an agency Center of Excellence, her firm works with prominent international clients including Bahamasair, Philips Semiconductors, Xerox Corporation, and World Airways on a variety of reputation management and communications assignments.

BETTY A. KILDOW, CBCP, FBCI, has been an emergency management and business continuity consultant for more than fifteen years. As a Certified Business

Continuity Professional (CBCP) and a Fellow of the Business Continuity Institute (FBCI), she has developed emergency management courses for the American Management Association and the University of California, Berkeley Extension. Ms. Kildow is author of the book *Front Desk Security and Safety: An On-the-Job Guide to Handling Emergencies, Threats, and Unexpected Situations* (AMACOM Publishing, 2004). She has written numerous articles for professional publications in the United States and the United Kingdom, and is frequently called upon as a speaker.

MICHAEL SEESE, M.S., M.A., CISSP, is an assistant vice president in the Corporate Security Services division of National City Corporation of Cleveland, Ohio, specializing in information security policy development and privacy. Prior to his current assignment, Mr. Seese served NCC as a business contingency planning consultant. He holds a master's of science in information security, a master's of arts in psychology, and recently earned his CISSP. With over twenty years' experience as an IT professional and journalist, he has had numerous articles published in professional journals. Recent speaking engagements include NetSec 2004, CPM 2005 West, and infosecurity New York 2006. He can be reached at Michael.Seese@NationalCity.com or mail@MichaelSeese.com.

GEARY SIKICH is the author of *It Can't Happen Here: All Hazards Crisis Management Planning, Emergency Management Planning Handbook* (available in both English and Spanish), and *Integrated Business Continuity: Maintaining Resilience in Uncertain Times*. Mr. Sikich is the founder and a principal with Logical Management Systems, Corporation (www.logicalmanagement.com), based in Munster, Indiana. He has extensive experience in management consulting in a variety of fields. Mr. Sikich consults on a regular basis with companies worldwide on business continuity and crisis management issues. He has a bachelor's of science degree in criminology from Indiana State University and a master's of education in counseling and guidance from the University of Texas, El Paso.

KRISTA VARNEY is a security program coordinator in the Corporate Security Services (CSS) division of National City Corporation. The CSS division incorporates both physical and logical security. She started her career in the Information Services division of National City and has spent the past several years in the Security division, specializing in ISO 27001 and 17799. She holds an undergraduate degree from Miami University (Ohio) and a master's of business administration from Baldwin Wallace College. In addition, Ms. Varney is a Certified Information Systems Security Professional (CISSP) and Project Management Professional (PMP). Ms. Varney was also a speaker at the RSA Conference in 2006 and 2007.