

Corporate Computer Security

Fifth Edition

Randall J. Boyle

Longwood University

Raymond R. Panko

University of Hawai`i at Mānoa



Director of Product Management: Linea Rowe
Product Management Lead, IT/MIS: Marcus Scherer
Product Manager, IT/MIS: Becca Golden
Senior Analyst, HE Content IT/MIS: Allie D'Aprile
Analyst, HE Content, Careers & Professional: Bridget Daly
Manager Content HE, Careers & Professional: Jenifer Niles
Director, Digital Studio & Content Production: Brian Hyland
Digital Producer: Tanika Henderson
Senior Digital Producer: Jaimie Noy
Managing Content Producer: Jennifer Sargunar

Content Producer (Team Lead): Faraz Sharique Ali
Assistant Content Producer: Rudrani Mukherjee
Manager, Rights & Permission, Higher Education: Annette Linder
Cover Designer: SPi Global
Cover Photo: EtiAmmos/Shutterstock
Full-Service Project Management: Integra Software Services Pvt. Ltd.
Full-Service Project Manager: Gowthaman Sadhanandham
Manufacturing Buyer: LSC Communications
Text Printer/Bindery: LSC Communications
Cover Printer: Phoenix Color
Text Font: Palatino LT Pro, 9.5/13

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on the appropriate page within text.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Copyright © 2021, 2015, 2013 by Pearson Education, Inc. or its affiliates. All Rights Reserved. Manufactured in the United States of America. This publication is protected by copyright, and permission should be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights and Permissions department, please visit www.pearsoned.com/permissions/.

Acknowledgments of third-party content appear on the appropriate page within the text.

PEARSON, ALWAYS LEARNING, and MYLAB MIS™ are exclusive trademarks owned by Pearson Education, Inc. or its affiliates in the U.S. and/or other countries.

Unless otherwise indicated herein, any third-party trademarks that may appear in this work are the property of their respective owners, and any references to third-party trademarks, logos, or other trade dress are for demonstrative or descriptive purposes only.

Such references are not intended to imply any sponsorship, endorsement, authorization, or promotion of Pearson's products by the owners of such marks, or any relationship between the owner and Pearson Education, Inc. or its affiliates, authors, licensees, or distributors.

Library of Congress Cataloging-in-Publication Data on File

Names: Panko, Raymond R., author. | Boyle, Randall, author.

Title: Corporate computer security / Randall J Boyle, Longwood University, Raymond R Panko, University of Hawai'i at Mānoa.

Other titles: Corporate computer and network security

Description: Fifth edition. | Boston : Pearson, 2021. | Panko's name appears alone on an earlier edition which bears the title: Corporate computer and network security. | Includes bibliographical references and index.

Identifiers: LCCN 2019039707 | ISBN 9780135822784 (paperback) | ISBN 0135822785 (paperback)

Subjects: LCSH: Business enterprises--Computer networks--Security measures. | Computer security. | Computer networks--Security measures. | Computer crimes--Prevention.

Classification: LCC QA76.9.A25 P36 2021 | DDC 005.8--dc23

LC record available at <https://lcn.loc.gov/2019039707>

ScoutAutomatedPrintCode



ISBN 10: 0-13-582278-5
ISBN 13: 978-0-13-582278-4

To Courtney, Noah, Fiona, Layla, and Henry.

—Randy Boyle

*To Julia Panko, my long-time networking and security editor and one of the best technology
minds I've ever encountered.*

—Ray Panko

Brief Contents

1	The Threat Environment	1
2	Planning and Policy	47
3	Cryptography	108
4	Secure Networks	167
5	Access Control	216
6	Firewalls	277
7	Host Hardening	327
8	Application Security	375
9	Data Protection	422
10	Incident and Disaster Response	473
Module A	Networking Concepts	520

Contents

Preface	xv		
About the Authors	xx		
1 The Threat Environment			
1.1 Introduction			
Basic Security Terminology			
THE THREAT ENVIRONMENT	1		
GOALS	3		
COMPROMISES	4		
COUNTERMEASURES	4		
1.2 Data Breaches			
COST OF DATA BREACHES	5		
SIZE OF DATA BREACHES	5		
Why Do Data Breaches Happen?			
How Do Data Breaches Happen?			
Case Study: The Target Data Breach			
HOW DID THEY DO IT?	7		
THE DAMAGE	8		
In the News			
1.3 Employee and Ex-Employee Threats			
Why Employees Are Dangerous			
Employee Sabotage			
Employee Hacking			
Employee Financial Theft and Theft of Intellectual Property	13		
Employee Extortion	14		
Employee Sexual or Racial Harassment	14		
Employee Computer and Internet Abuse	14		
INTERNET ABUSE	14		
NON-INTERNET COMPUTER ABUSE	15		
Unintentional Data Loss	15		
Other “Internal” Attackers	15		
1.4 Malware			
Malware Writers			
Viruses			
Worms			
Ransomware			
Blended Threats			
Payloads			
Trojan Horses and Rootkits			
NONMOBILE MALWARE	18		
TROJAN HORSES	18		
REMOTE ACCESS TROJANS	19		
DOWNLOADERS	19		
SPYWARE	20		
ROOTKITS	20		
Mobile Code	21		
Social Engineering in Malware	21		
SPAM	21		
PHISHING	21		
SPEAR PHISHING	22		
HOAXES	22		
1.5 Hackers and Attacks			
Traditional Motives	22		
Anatomy of a Hack	24		
TARGET SELECTION	24		
RECONNAISSANCE PROBES	24		
THE EXPLOIT	25		
SPOOFING	25		
Social Engineering in an Attack	26		
Denial-of-Service Attacks	27		
Skill Levels	28		
1.6 The Criminal Era			29
Dominance by Career Criminals			29
CYBERCRIME	30		
INTERNATIONAL GANGS	31		
ADVANCED PERSISTENT THREATS	31		
BLACK MARKETS AND MARKET SPECIALIZATION	31		
Fraud, Theft, and Extortion			32
FRAUD	32		
FINANCIAL AND INTELLECTUAL PROPERTY THEFT	32		
EXTORTION AGAINST CORPORATIONS	33		
Stealing Sensitive Data about Customers and Employees			33
CARDING	33		
BANK ACCOUNT THEFT	33		
IDENTITY THEFT	33		
THE CORPORATE CONNECTION	34		
CORPORATE IDENTITY THEFT	34		
1.7 Competitor Threats			35
Commercial Espionage			35
Denial-of-Service Attacks			36
1.8 Cyberwar and Cyberterror			36
Cyberwar			36
Cyberterror			37
1.9 Conclusion			38
Security @ Work: Equihax			39
Security Technology: Going Phishing			40
Security Ethics: The Lure of Love Bots			42
Thought Questions	44		
Hands-On Projects	44		
Project Thought Questions	45		
Case Discussion Questions	46		
Perspective Questions	46		
2 Planning and Policy			47
2.1 Introduction			47
Defense			47
Management Processes			48
MANAGEMENT IS THE HARD PART	49		
COMPREHENSIVE SECURITY	49		
WEAKEST-LINKS FAILURES	49		
THE NEED TO PROTECT MANY RESOURCES	50		
The Need for a Disciplined Security Management Process			50
The Plan–Protect–Respond Cycle			51
PLANNING	51		
PROTECTION	51		
RESPONSE	52		
Vision in Planning			53
VIEWING SECURITY AS AN ENABLER	53		
DEVELOPING POSITIVE VISIONS OF USERS	54		
Strategic IT Security Planning			55
In the News			56
2.2 Compliance Laws and Regulations			58
Driving Forces			58
Sarbanes–Oxley			58
Privacy Protection Laws			60
Data Breach Notification Laws			60
The Federal Trade Commission			61
Industry Accreditation			61
PCI-DSS			61
FISMA			61

2.3 Organization

Chief Security Officers

Should You Place Security within IT?

LOCATING SECURITY WITHIN IT 64 • PLACING SECURITY
OUTSIDE IT 64 • A HYBRID SOLUTION 64

Top Management Support

Relationships with Other Departments

SPECIAL RELATIONSHIPS 65 • ALL CORPORATE
DEPARTMENTS 66 • BUSINESS PARTNERS 66

Outsourcing IT Security

E-MAIL OUTSOURCING 66 • MANAGED SECURITY
SERVICE PROVIDER 67**2.4 Risk Analysis**

Reasonable Risk

Classic Risk Analysis Calculations

ASSET VALUE 69 • EXPOSURE FACTOR 69 • SINGLE
LOSS EXPECTANCY 69 • ANNUALIZED PROBABILITY
(OR RATE) OF OCCURRENCE 69 • ANNUALIZED
LOSS EXPECTANCY 69 • COUNTERMEASURE
IMPACT 70 • ANNUALIZED COUNTERMEASURE COST
AND NET VALUE 70

Problems with Classic Risk Analysis Calculations

UNEVEN MULTIYEAR CASH FLOWS 71 •
TOTAL COST OF INCIDENT 71 • MANY-TO-MANY
RELATIONSHIPS BETWEEN COUNTERMEASURES AND
RESOURCES 71 • THE IMPOSSIBILITY OF COMPUTING
ANNUALIZED RATES OF OCCURRENCE 71 •
THE PROBLEM WITH “HARD-HEADED
THINKING” 72 • PERSPECTIVE 73

Responding to Risk

RISK REDUCTION 73 • RISK ACCEPTANCE 73 • RISK
TRANSFERENCE (INSURANCE) 73 • RISK AVOIDANCE 73**2.5 Technical Security Architecture**

Technical Security Architectures

ARCHITECTURAL DECISIONS 75 • DEALING WITH
LEGACY SECURITY TECHNOLOGY 75

Principles

DEFENSE IN DEPTH 75 • DEFENSE IN DEPTH VERSUS
WEAKEST LINKS 75 • SINGLE POINTS OF
VULNERABILITY 76 • MINIMIZING SECURITY
BURDENS 77 • REALISTIC GOALS 77

Elements of a Technical Security Architecture

BORDER MANAGEMENT 78 • INTERNAL SITE
SECURITY MANAGEMENT 78 • MANAGEMENT OF
REMOTE CONNECTIONS 78 • INTERORGANIZATIONAL
SYSTEMS 78 • CENTRALIZED SECURITY
MANAGEMENT 78**2.6 Policy-Driven Implementation**

Policies

WHAT ARE POLICIES? 79 • WHAT, NOT HOW 79 • CLARITY 79

Categories of Security Policies

CORPORATE SECURITY POLICY 80 • MAJOR
POLICIES 80 • ACCEPTABLE USE POLICY 81 • POLICIES
FOR SPECIFIC COUNTERMEASURES OR RESOURCES 81

Policy-Writing Teams

62 Implementation Guidance 81

62 NO GUIDANCE 82 • STANDARDS AND GUIDELINES 83

63 Types of Implementation Guidance 83

PROCEDURES 83 • PROCESSES 84 •
BASELINES 84 • BEST PRACTICES AND RECOMMENDED
PRACTICES 84 • ACCOUNTABILITY 85 •
ETHICS 85

64 Exception Handling 86

65 Oversight 87

POLICIES AND OVERSIGHT 88 • PROMULGATION 88
• ELECTRONIC MONITORING 88 • SECURITY METRICS 88
• AUDITING 89 • ANONYMOUS PROTECTED HOTLINE 89
• BEHAVIORAL AWARENESS 91 • FRAUD 91 • SANCTIONS 92

68 Federal Surveillance Laws 93

68 DOMESTIC SURVEILLANCE LAWS 94

69 **2.7 Governance Frameworks** 95

69 COSO 96

THE COSO FRAMEWORK 96 • OBJECTIVES 96 •
REASONABLE ASSURANCE 96 • COSO FRAMEWORK
COMPONENTS 96

COBIT 98

THE COBIT FRAMEWORK 98 • DOMINANCE IN THE UNITED
STATES 99

71 The ISO/IEC 27000 Series 99

ISO/IEC 27002 99 • ISO/IEC 27001 100
OTHER 27000 STANDARDS 10071 **2.8 Conclusion** 10071 **Security @ Work: Security in the Sharing Economy** 10171 **Security Technology: Top 10 Application** 10171 **Vulnerabilities** 10371 **Security Ethics: Securing Privacy** 10371 **Thought Questions** 105 • **Hands-on Projects** 10571 • **Project Thought Questions** 10671 • **Case Discussion Questions** 10771 • **Perspective Questions** 107**3 Cryptography** 10875 **3.1 What Is Cryptography?** 108

75 Encryption for Confidentiality 109

75 Terminology 109

PLAINTEXT 109 • ENCRYPTION AND
CIPHERTEXT 110 • CIPHER 110 • KEY 110 •
KEEPING THE KEY SECRET 110

75 The Simple Cipher 110

75 Cryptanalysis 111

75 Substitution and Transposition Ciphers 112

75 Substitution Ciphers 112

75 Transposition Ciphers 112

75 Real-World Encryption 112

75 Ciphers and Codes 113

75 Symmetric Key Encryption 114

KEY LENGTH 114

75 Human Issues in Cryptography 116

81 **In the News** 116

3.2 Symmetric Key Encryption Ciphers	118	3.8 Quantum Security	143
RC4	118	3.9 Cryptographic Systems	144
The Data Encryption Standard (DES)	119	Virtual Private Networks (VPNs)	145
56-BIT KEY SIZE 119 • BLOCK ENCRYPTION 119		Why VPNs?	146
Triple DES (3DES)	120	Host-to-Host VPNs	146
168-BIT 3DES OPERATION 120 • 112-BIT 3DES 120 • PERSPECTIVE ON 3DES 120		Remote Access VPNs	146
Advanced Encryption Standard (AES)	120	Site-to-Site VPNs	146
Other Symmetric Key Encryption Ciphers	121	3.10 SSL/TLS	147
3.3 Cryptographic System Standards	122	Nontransparent Protection	147
Cryptographic Systems	122	Inexpensive Operation	148
Initial Handshaking Stages	122	SSL/TLS Gateways and Remote Access VPNs	148
NEGOTIATION 122 • INITIAL AUTHENTICATION 123 • KEYING 123		VPN GATEWAY STANDARDS 148 • AUTHENTICATION 149	
Ongoing Communication	123	• CONNECTING THE CLIENT PC TO AUTHORIZED RESOURCES 149 • SECURITY FOR SERVICES 150 • BROWSER ON THE CLIENT 150 • ADVANCED SERVICES REQUIRE ADMINISTRATOR PRIVILEGES ON PCS 150 • PERSPECTIVE 150	
3.4 The Negotiation Stage	124	3.11 IPsec	151
Cipher Suite Options	124	Attractions of IPsec	151
Cipher Suite Policies	125	SSL/TLS GIVES NONTRANSPARENT TRANSPORT LAYER SECURITY 152 • IPSEC: TRANSPARENT INTERNET LAYER SECURITY 152 • IPSEC IN BOTH IPV4 AND IPV6 152	
3.5 Initial Authentication Stage	125	IPsec Transport Mode	152
Authentication Terminology	125	HOST-TO-HOST SECURITY 153 • END-TO-END PROTECTION 153 • COST OF SETUP 153 • IPSEC IN TRANSPORT MODE AND FIREWALLS 154	
Hashing	126	IPsec Tunnel Mode	154
Initial Authentication with MS-CHAP	127	PROTECTION IS PROVIDED BY IPSEC GATEWAYS 154 • LESS EXPENSIVE THAN TRANSPORT MODE 154 • FIREWALL-FRIENDLY PROTECTION 154 • NO PROTECTION WITHIN THE TWO SITES 154	
ON THE SUPPLICANT'S MACHINE: HASHING 127 • ON THE VERIFIER SERVER 127		IPsec Security Associations (SAs)	155
3.6 The Keying Stage	129	SEPARATE SAS IN THE TWO DIRECTIONS 155 • POLICY-BASED SA 155	
Session Keys	129	3.12 Conclusion	156
Public Key Encryption for Confidentiality	129	Security @ Work: Social Engineering Bitcoin	158
TWO KEYS 129 • PROCESS 129 • PADLOCK AND KEY ANALOGY 130 • HIGH COST AND SHORT MESSAGE LENGTHS 130 • RSA AND ECC 130 • KEY LENGTH 130		Security Technology: Kryptos	160
Symmetric Key Keying Using Public Key Encryption	131	Security Ethics: Reverse Engineering Privacy	161
Symmetric Key Keying Using Diffie–Hellman Key Exchange	132	Thought Questions 163 • Hands-on Projects 163 • Project Thought Questions 164 • Case Discussion Questions 166 • Perspective Questions 166	
3.7 Message-by-Message Authentication	133	4 Secure Networks	167
Electronic Signatures	133	4.1 Introduction	167
Public Key Encryption for Authentication	134	Creating Secure Networks	167
Message-by-Message Authentication with Digital Signatures	134	AVAILABILITY 168 • CONFIDENTIALITY 168 • FUNCTIONALITY 168 • ACCESS CONTROL 168	
DIGITAL SIGNATURES 135 • HASHING TO PRODUCE THE MESSAGE DIGEST 135 • SIGNING THE MESSAGE DIGEST TO PRODUCE THE DIGITAL SIGNATURE 135 • SENDING THE MESSAGE WITH CONFIDENTIALITY 136 • VERIFYING THE SUPPLICANT • MESSAGE INTEGRITY 136 • PUBLIC KEY ENCRYPTION FOR CONFIDENTIALITY AND AUTHENTICATION 136		Future of Secure Networks	169
Digital Certificates	137	DEATH OF THE PERIMETER 169 • RISE OF THE CITY 170	
CERTIFICATE AUTHORITIES 137 • DIGITAL CERTIFICATE 138 • VERIFYING THE DIGITAL CERTIFICATE 139 • THE ROLES OF THE DIGITAL CERTIFICATE AND DIGITAL SIGNATURE 140		In the News	170
Key-Hashed Message Authentication Codes	141	4.2 DoS Attacks	171
THE PROBLEM WITH DIGITAL SIGNATURES 141		Denial of Service. . .But Not an Attack	171
Creating and Testing the HMAC	141	FAULTY CODING 172 • REFERRALS FROM LARGE SITES 172	
Nonrepudiation	143	Goal of DoS Attacks	172
		STOP CRITICAL SERVICES 172 • DEGRADE SERVICES 172	

Methods of DoS Attacks		
DIRECT AND INDIRECT ATTACKS 174 •		
INTERMEDIARY 175 • REFLECTED ATTACK 178 •		
SENDING MALFORMED PACKETS 179		
Defending against Denial-of-Service Attacks	180	
BLACK HOLING 180 • VALIDATING THE HANDSHAKE 180		
• RATE LIMITING 180		
4.3 ARP Poisoning	181	
Normal ARP Operation	183	
THE PROBLEM 183		
ARP Poisoning	184	
ARP DoS Attack	185	
Preventing ARP Poisoning	185	
STATIC TABLES 185 • LIMIT LOCAL ACCESS 186		
4.4 Access Control for Networks	186	
LAN Connections	187	
Access Control Threats	187	
Eavesdropping Threats	187	
4.5 Ethernet Security	188	
Ethernet and 802.1X	188	
COST SAVINGS 189 • CONSISTENCY 189 • IMMEDIATE		
CHANGES 189		
The Extensible Authentication Protocol (EAP)	189	
EAP OPERATION 189 • EXTENSIBILITY 190		
RADIUS Servers	191	
RADIUS AND EAP 192		
4.6 Wireless Security	192	
Wireless Attacks	192	
Unauthorized Network Access	193	
PREVENTING UNAUTHORIZED ACCESS 193		
Evil Twin Access Points	195	
Wireless Denial of Service	196	
FLOOD THE FREQUENCY 197 • FLOOD THE ACCESS		
POINT 197 • SEND ATTACK COMMANDS 197		
Wireless LAN Security with 802.11i	198	
EAP'S NEED FOR SECURITY 198 • ADDING SECURITY		
TO EAP 199 • EAP-TLS AND PEAP 200		
Core Wireless Security Protocols	200	
Wired Equivalent Privacy (WEP)	200	
Cracking WEP	201	
SHARED KEYS AND OPERATIONAL SECURITY 201 •		
EXPLOITING WEP'S WEAKNESS 201		
Perspective	202	
Wi-Fi Protected Access (WPA™)	203	
Pre-Shared Key (PSK) Mode	204	
Wireless Intrusion Detection Systems	205	
False 802.11 Security Measures	206	
SPREAD SPECTRUM OPERATION AND SECURITY 206 •		
TURNING OFF SSID BROADCASTING 207 • MAC ACCESS		
CONTROL LISTS 207		
Implementing 802.11i or WPA Is Easier	207	
4.7 Conclusion	208	
Security @ Work: Anthem to Anathema	209	
Security Technology: IoT and Mirai	210	
Security Ethics: Mining at Work	211	
Thought Questions 213 • Hands-on Projects 213 • Project	173	
Thought Questions 214 • Case Discussion Questions 215 •		
Perspective Questions 215		
5 Access Control	216	
5.1 Introduction	216	
Access Control	216	
Authentication, Authorizations, and Auditing	217	
Authentication	217	
Beyond Passwords	217	
Two-Factor Authentication	217	
Individual and Role-Based Access Control	218	
Organizational and Human Controls	219	
Military and National Security Organization		
Access Controls	219	
Multilevel Security	220	
In the News	221	
5.2 Physical Access and Security	222	
Risk Analysis	222	
ISO/IEC 11.1: Secure Areas	222	
PHYSICAL SECURITY PERIMETER 222 • PHYSICAL ENTRY		
CONTROLS 223 • SECURING OFFICES, ROOMS, AND		
FACILITIES 223 • PROTECTING AGAINST EXTERNAL AND		
ENVIRONMENTAL THREATS 223 • RULES FOR WORKING IN		
SECURE AREAS 224 • PUBLIC ACCESS, DELIVERY, AND LOADING		
AREAS 224		
ISO/IEC 11.2 Equipment Security	224	
EQUIPMENT SITING AND PROTECTION 224 • SUPPORTING		
UTILITIES 225 • CABLING SECURITY 225 • SECURITY DURING		
OFF-SITE EQUIPMENT MAINTENANCE 225 • REMOVAL		
OF PROPERTY 225 • SECURITY OF EQUIPMENT OFF-		
PREMISES 225 • SECURE DISPOSAL OR REUSE OF		
EQUIPMENT 225 • CLEAR DESK AND CLEAR SCREEN 226		
Other Physical Security Issues	226	
TERRORISM 226 • PIGGYBACKING 226 • MONITORING		
EQUIPMENT 226 • DUMPSTERS 227 • DESKTOP PC		
SECURITY 227 • NOTEBOOK SECURITY 228		
5.3 Passwords	228	
Password-Cracking Programs	228	
Password Policies	228	
Password Use and Misuse	229	
NOT USING THE SAME PASSWORD AT MULTIPLE		
SITES 229 • PASSWORD DURATION POLICIES 229 • POLICIES		
PROHIBITING SHARED ACCOUNTS 229 • DISABLING		
PASSWORDS THAT ARE NO LONGER VALID 230 • LOST		
PASSWORDS 231 • PASSWORD STRENGTH 232 • PASSWORD		
AUDITING 232		
The End of Passwords?	234	
5.4 Access Cards and Tokens	234	
Access Cards	234	
MAGNETIC STRIPE CARDS 235 • SMART CARDS 236 •		
CARD READER COSTS 236		
Tokens	236	
ONE-TIME-PASSWORD TOKENS 236 • USB TOKENS 236		
Proximity Access Tokens	236	
Addressing Loss and Theft	236	
PHYSICAL DEVICE CANCELLATION 237 • TWO-FACTOR		
AUTHENTICATION 237		

5.5 Biometric Authentication	238	Security @ Work: IRS Overtaxed	269
Biometrics	238	Security Technology: Lock Picking and Viral Videos	270
Biometric Systems	238	Security Ethics: Web Recording—Everything	272
INITIAL ENROLLMENT 238 • SUBSEQUENT ACCESS ATTEMPTS 240 • ACCEPTANCE OR REJECTION 240		Thought Questions 273 • Hands-on Projects 274 • Project Thought Questions 275 • Case Discussion Questions 276 • Perspective Questions 276	
Biometric Errors	240	6 Firewalls	277
FALSE ACCEPTANCE RATE 241 • FALSE REJECTION RATE 241 • WHICH IS WORSE? 241 • VENDOR CLAIMS 241 • FAILURE TO ENROLL 242		6.1 Introduction	277
Verification, Identification, and Watch Lists	242	Basic Firewall Operation	277
VERIFICATION 242 • IDENTIFICATION 243 • WATCH LISTS 244		The Danger of Traffic Overload	279
Biometric Deception	244	Firewall Filtering Mechanisms	280
Biometric Methods	245	In the News	281
FINGERPRINT RECOGNITION 245 • IRIS RECOGNITION 246 • FACE RECOGNITION 247 • HAND GEOMETRY 247 • VOICE RECOGNITION 247 • OTHER FORMS OF BIOMETRIC AUTHENTICATION 248		6.2 Static Packet Filtering	282
5.6 Cryptographic Authentication	248	Looking at Packets One at a Time	282
Key Points from Chapter 3	248	Looking Only at Some Fields in the Internet and Transport Headers	282
Public Key Infrastructures	249	Usefulness of Static Packet Filtering	282
THE FIRM AS A CERTIFICATE AUTHORITY 249 • CREATING PUBLIC KEY–PRIVATE KEY PAIRS 249 • DISTRIBUTING DIGITAL CERTIFICATES 249 • ACCEPTING DIGITAL CERTIFICATES 250 • CERTIFICATE REVOCATION STATUS 250 • PROVISIONING 250 • THE PRIME AUTHENTICATION PROBLEM 250		Perspective	283
5.7 Authorization	251	6.3 Stateful Packet Inspection	284
The Principle of Least Permissions	251	Basic Operation	284
5.8 Auditing	253	CONNECTIONS 284 • STATES 284 • STATEFUL PACKET INSPECTION WITH TWO STATES 285 • REPRESENTING CONNECTIONS 286	
Logging	253	Packets That Do Not Attempt to Open Connections	286
Log Reading	253	TCP CONNECTIONS 286 • UDP AND ICMP CONNECTIONS 287 • ATTACK ATTEMPTS 287 • PERSPECTIVE 288	
REGULAR LOG READING 253 • PERIODIC EXTERNAL AUDITS OF LOG FILE ENTRIES 253 • AUTOMATIC ALERTS 254		Packets That Do Attempt to Open a Connection	288
5.9 Central Authentication Servers	254	Access Control Lists (ACLs) for Connection-Opening Attempts	288
The Need for Centralized Authentication	254	WELL-KNOWN PORT NUMBERS 289 • ACCESS CONTROL LISTS FOR INGRESS FILTERING 289 • IF-THEN FORMAT 289 • PORTS AND SERVER ACCESS 290 • DISALLOW ALL CONNECTIONS 290	
Kerberos	255	Perspective on SPI Firewalls	292
5.10 Directory Servers	256	LOW COST 292 • SAFETY 292 • DOMINANCE 292	
What Are Directory Servers?	257	6.4 Network Address Translation	292
Hierarchical Data Organization	257	Sniffers	292
Lightweight Data Access Protocol	258	NAT OPERATION 292 • PACKET CREATION 292 • NETWORK AND PORT ADDRESS TRANSLATION (NAT/PAT) 293 • TRANSLATION TABLE 293 • RESPONSE PACKET 293 • RESTORATION 293 • PROTECTION 293	
Use by Authentication Servers	258	Perspective on NAT	293
Active Directory	258	NAT/PAT 293 • TRANSPARENCY 294 • NAT TRAVERSAL 294	
ACTIVE DIRECTORY DOMAINS 259		6.5 Application Proxy Firewalls and Content Filtering	294
Trust	260	Application Proxy Firewall Operation	294
5.11 Full Identity Management	261	APPLICATION PROXY PROGRAMS VERSUS APPLICATION PROXY FIREWALLS 294 • PROCESSING-INTENSIVE OPERATION 294 • ONLY A FEW APPLICATIONS CAN BE PROXIED 295 • TWO COMMON USES 295	
Other Directory Servers and Metadirectories	261	Application Content Filtering in Stateful Packet Inspection Firewalls	296
Federated Identity Management	262	Application Content Filtering for HTTP	297
THE SECURITY ASSERTION MARKUP LANGUAGE 263 • PERSPECTIVE 263		Client Protections	298
Identity Management	263		
BENEFITS OF IDENTITY MANAGEMENT 264 • WHAT IS IDENTITY? 264 • IDENTITY MANAGEMENT 265			
Trust and Risk	266		
5.12 Conclusion	267		

X Contents

Server Protections	298	Thought Questions	323	Hands-on Projects	323	Project	
Other Protections	298	Thought Questions	325	Case Discussion Questions	326	Perspective Questions	326
6.6 Intrusion Detection Systems and Intrusion Prevention Systems	299	7 Host Hardening					327
Intrusion Detection Systems	299	7.1 Introduction					327
FIREWALLS VERSUS IDSS 299 • FALSE POSITIVES (FALSE ALARMS) 300 • HEAVY PROCESSING REQUIREMENTS 301		What Is a Host?					327
Intrusion Prevention Systems	301	The Elements of Host Hardening					327
ASICS FOR FASTER PROCESSING 301 • THE ATTACK IDENTIFICATION CONFIDENCE SPECTRUM 302		Security Baselines and Images					328
IPS Actions	302	Virtualization					329
DROPPING PACKETS 302 • LIMITING TRAFFIC 302		VIRTUALIZATION ANALOGY 330 • BENEFITS OF VIRTUALIZATION 331					
6.7 Antivirus Filtering and Unified Threat Management	302	Systems Administrators					331
6.8 Firewall Architectures	304	In the News					332
Main Border Firewalls	304	7.2 Important Server Operating Systems					333
Screening Border Routers	304	Windows Server Operating Systems					333
Internal Firewalls	304	THE WINDOWS SERVER USER INTERFACE 334 • START → ADMINISTRATIVE TOOLS 334 • WINDOWS SERVER MANAGER 334 • MICROSOFT MANAGEMENT CONSOLES (MMC) 334					
Host Firewalls	304	UNIX (Including Linux) Servers					336
DEFENSE IN DEPTH 305		MANY VERSIONS 336 • LINUX 337 • UNIX DESKTOP ENVIRONMENTS 337					
The Demilitarized Zone (DMZ)	305	7.3 Vulnerabilities and Patches					339
SECURITY IMPLICATIONS 306 • HOSTS IN THE DMZ 306		Vulnerabilities and Exploits					339
6.9 Firewall Management	307	Fixes					339
Defining Firewall Policies	307	WORK-AROUNDS 339 • PATCHES 339 • SERVICE PACKS 340 • VERSION UPGRADES 340					
WHY USE POLICIES? 307 • EXAMPLES OF POLICIES 307		The Mechanics of Patch Installation					341
Implementation	307	MICROSOFT WINDOWS SERVER 341 • LINUX RPM PROGRAM 341					
FIREWALL HARDENING 307 • CENTRAL FIREWALL MANAGEMENT SYSTEMS 309 • FIREWALL POLICY DATABASE 309 • VULNERABILITY TESTING AFTER CONFIGURATION 310 • CHANGE AUTHORIZATION AND MANAGEMENT 310 • READING FIREWALL LOGS 311		Problems with Patching					341
Understanding How to Read Firewall Logs	312	THE NUMBER OF PATCHES 341 • COST OF PATCH INSTALLATION 341 • PRIORITIZING PATCHES 341 • PATCH MANAGEMENT SERVERS 343 • THE RISKS OF PATCH INSTALLATION 343					
Log Files	312	7.4 Managing Users and Groups					343
Sorting the Log File by Rule	312	The Importance of Groups in Security Management					343
Echo Probes	313	Creating and Managing Users and Groups in Windows					344
External Access to All Internal FTP Servers	313	THE ADMINISTRATOR ACCOUNT 344 • MANAGING ACCOUNTS 344 • CREATING USERS 344 • WINDOWS GROUPS 344					
Attempted Access to Internal Webservers	313	7.5 Managing Permissions					346
Incoming Packet with a Private IP Source Address	313	Permissions					346
Lack of Capacity	314	Assigning Permissions in Windows					347
Perspective	314	DIRECTORY PERMISSIONS 347 • WINDOWS PERMISSIONS 347 • ADDING USERS AND GROUPS 347 • INHERITANCE 347 • DIRECTORY ORGANIZATION 348					
Sizes of Log Files	314	Assigning Groups and Permissions in UNIX					348
Logging All Packets	314	NUMBER OF PERMISSIONS 349 • NUMBER OF ACCOUNTS OR GROUPS 349					
6.10 Firewall Filtering Problems	315	7.6 Creating Strong Passwords					349
The Death of the Perimeter	315	Creating and Storing Passwords					350
AVOIDING THE BORDER FIREWALL 315 • EXTENDING THE PERIMETER 316 • PERSPECTIVE 316		CREATING A PASSWORD HASH 350 • STORING PASSWORDS 350 • STEALING PASSWORDS 351					
Attack Signatures versus Anomaly Detection	316						
ZERO-DAY ATTACKS 317 • ANOMALY DETECTION 317 • ACCURACY 317							
6.11 Conclusion	317						
Security @ Work: Watching the Watchers	319						
Security Technology: Tor—Onion Routing	320						
Security Ethics: Privacy versus Productivity: The BYOD Dilemma	322						

<ul style="list-style-type: none"> Password-Cracking Techniques 351 <ul style="list-style-type: none"> BRUTE-FORCE GUESSING 351 • DICTIONARY ATTACKS ON COMMON WORD PASSWORDS 353 • HYBRID DICTIONARY ATTACKS 353 • RAINBOW TABLES 354 • TRULY RANDOM PASSWORDS 355 • TESTING AND ENFORCING THE STRENGTH OF PASSWORDS 355 • OTHER PASSWORD THREATS 355 7.7 Testing for Vulnerabilities 356 Windows Client PC Security 357 Client PC Security Baselines 357 The Windows Security Application 357 Windows Defender Firewall 358 Automatic Updates 359 Antivirus and Spyware Protection 360 Implementing Security Policy 360 <ul style="list-style-type: none"> PASSWORD POLICIES 360 • ACCOUNT POLICIES 360 • AUDIT POLICIES 361 Protecting Notebook Computers 362 <ul style="list-style-type: none"> THREATS 362 • BACKUP 362 • POLICIES FOR SENSITIVE DATA 362 • TRAINING 363 • ANTI-THEFT TRACKING SOFTWARE 363 Centralized PC Security Management 363 <ul style="list-style-type: none"> STANDARD CONFIGURATIONS 363 • NETWORK ACCESS CONTROL 364 • WINDOWS GROUP POLICY OBJECTS 364 7.8 Conclusion 366 Security @ Work: Hacking Smart Things 367 Security Technology: Antivirus Industry 369 Security Ethics: MIS-Diagnosis 370 Thought Questions 371 • Hands-on Projects 371 • Project Thought Questions 372 • Case Discussion Questions 373 • Perspective Questions 374 	<ul style="list-style-type: none"> 8 Application Security 375 8.1 Application Security and Hardening 375 Executing Commands with the Privileges of a Compromised Application 375 Buffer Overflow Attacks 376 <ul style="list-style-type: none"> BUFFERS AND OVERFLOWS 376 • STACKS 376 • RETURN ADDRESS 376 • THE BUFFER AND BUFFER OVERFLOW 376 • EXECUTING ATTACK CODE 376 • AN EXAMPLE: THE IIS IPP BUFFER OVERFLOW ATTACK 377 Few Operating Systems, Many Applications 378 Hardening Applications 378 <ul style="list-style-type: none"> UNDERSTAND THE SERVER'S ROLE AND THREAT ENVIRONMENT 378 • THE BASICS 378 • MINIMIZE APPLICATIONS 378 • SECURITY BASELINES FOR APPLICATION MINIMIZATION 380 • CREATE A SECURE CONFIGURATION 380 • INSTALL APPLICATION PATCHES AND UPDATES 380 • MINIMIZE THE PERMISSIONS OF APPLICATIONS 380 • ADD APPLICATION-LEVEL AUTHENTICATION, AUTHORIZATIONS, AND AUDITING 380 • IMPLEMENT CRYPTOGRAPHIC SYSTEMS 381 Securing Custom Applications 381 <ul style="list-style-type: none"> NEVER TRUST USER INPUT 381 • BUFFER OVERFLOW ATTACKS 381 • LOGIN SCREEN BYPASS ATTACKS 381 • CROSS-SITE SCRIPTING ATTACKS 382 • SQL INJECTION ATTACKS 383 • AJAX MANIPULATION 386 • TRAINING IN SECURE COMPUTING 386 In the News 386 8.2 WWW and E-Commerce Security 388 The Importance of WWW and E-commerce Security 388 WWW Service versus E-commerce Service 388 <ul style="list-style-type: none"> WWW SERVICE 388 • E-COMMERCE SERVICE 389 • EXTERNAL ACCESS 389 • CUSTOM PROGRAMS 390 Some Webserver Attacks 390 <ul style="list-style-type: none"> WEBSITE DEFAACEMENT 390 • BUFFER OVERFLOW ATTACK TO LAUNCH A COMMAND SHELL 390 • DIRECTORY TRAVERSAL ATTACK 390 • THE DIRECTORY TRAVERSAL WITH HEXADECIMAL CHARACTER ESCAPES 391 • UNICODE DIRECTORY TRAVERSAL 392 Patching the Webserver and E-commerce Software and Its Components 392 <ul style="list-style-type: none"> E-COMMERCE SOFTWARE VULNERABILITIES 392 Other Website Protections 393 <ul style="list-style-type: none"> WEBSITE VULNERABILITY ASSESSMENT TOOLS 393 • WEBSITE ERROR LOGS 393 • WEBSERVER-SPECIFIC APPLICATION PROXY FIREWALLS 394 Controlling Deployment 394 <ul style="list-style-type: none"> DEVELOPMENT SERVERS 394 • TESTING SERVERS 394 • PRODUCTION SERVERS 394 8.3 Web Browser Attacks 395 BROWSER THREATS 395 • MOBILE CODE 395 • MALICIOUS LINKS 397 • OTHER CLIENT-SIDE ATTACKS 397 Enhancing Browser Security 398 <ul style="list-style-type: none"> CONFIGURATION 398 • INTERNET OPTIONS 398 • SECURITY TAB 399 • PRIVACY TAB 399 8.4 E-Mail Security 399 E-mail Content Filtering 399 <ul style="list-style-type: none"> MALICIOUS CODE IN ATTACHMENTS AND HTML BODIES 400 • SPAM 400 • INAPPROPRIATE CONTENT 401 • EXTRUSION PREVENTION 401 • PERSONALLY IDENTIFIABLE INFORMATION 401 Where to Do E-mail Malware and Spam Filtering 401 E-mail Encryption 402 <ul style="list-style-type: none"> TRANSMISSION ENCRYPTION 402 • MESSAGE ENCRYPTION 403 8.5 Voice Over IP (VOIP) Security 404 Sending Voice between Phones 404 Transport and Signaling 405 SIP and H.323 405 Registration 405 SIP Proxy Servers 405 PSTN Gateway 406 VoIP Threats 406 Eavesdropping 406 Denial-of-Service Attacks 406 Caller Impersonation 407 Hacking and Malware Attacks 407 Toll Fraud 407 Spam over IP Telephony 408 New Threats 408 Implementing VoIP Security 408 Authentication 408
---	--

Encryption for Confidentiality 408

Firewalls 409

NAT Problems 409

Separation: Anticonvergence 410

The Skype VoIP Service 410

8.6 Other User Applications 411

Instant Messaging 411

TCP/IP Supervisory Applications 411

8.7 Conclusion 414

Security @ Work: Exhaustive Cheating 414

Security Technology: New from Black Hat 416

Security Ethics: Free Apps For Data 417

Thought Questions 419 • Hands-on Projects 419 • Project Thought Questions 420 • Case Discussion Questions 421 • Perspective Questions 421

9 Data Protection 422

9.1 Introduction 422

Data’s Role in Business 422

TARGET DATA BREACH 423

Securing Data 423

In the News 423

9.2 Data Protection: Backup 424

The Importance of Backup 424

Threats 424

Scope of Backup 425

FILE/DIRECTORY DATA BACKUP 425 • IMAGE BACKUP 425 • SHADOWING 426

Full versus Incremental Backups 427

Backup Technologies 428

LOCAL BACKUP 428 • CENTRALIZED BACKUP 429 • CONTINUOUS DATA PROTECTION 430 • INTERNET BACKUP SERVICE 430 • MESH BACKUP 430

9.3 Backup Media and RAID 431

MAGNETIC TAPE 431 • CLIENT PC BACKUP 431

Disk Arrays—RAID 432

Raid Levels 433

NO RAID 433 • RAID 0 433 • RAID 1 434 • RAID 5 435

9.4 Data Storage Policies 438

BACKUP CREATION POLICIES 438 • RESTORATION POLICIES 438 • MEDIA STORAGE LOCATION POLICIES 439 • ENCRYPTION POLICIES 439 • ACCESS CONTROL POLICIES 439 • RETENTION POLICIES 440 • AUDITING BACKUP POLICY COMPLIANCE 440

E-mail Retention 440

THE BENEFIT OF RETENTION 440 • THE DANGERS OF RETENTION 440 • ACCIDENTAL RETENTION 441 • THIRD-PARTY E-MAIL RETENTION 441 • LEGAL ARCHIVING REQUIREMENTS 441 • U.S. FEDERAL RULES OF CIVIL PROCEDURE 441 • MESSAGE AUTHENTICATION 443 • DEVELOPING POLICIES AND PROCESSES 443

User Training 443

Spreadsheets 444

Vault Server Access Control 444 • Other Vault Server Protections 445

9.5 Database Security 445

Relational Databases 446

LIMITING THE VIEW OF DATA 447

Database Access Control 449

DATABASE ACCOUNTS 449 • SQL INJECTION ATTACKS 449

Database Auditing 450

WHAT TO AUDIT 450 • TRIGGERS 451

Database Placement and Configuration 451

CHANGE THE DEFAULT PORT 452

Data Encryption 453

KEY ESCROW 454 • FILE/DIRECTORY ENCRYPTION VERSUS WHOLE-DISK ENCRYPTION 454 • PROTECTING ACCESS TO THE COMPUTER 454 • DIFFICULTIES IN FILE SHARING 454

9.6 Data Loss Prevention 455

Data Collection 455

PERSONALLY IDENTIFIABLE INFORMATION 455 • DATA MASKING 456

Information Triangulation 456

BUY OR SELL DATA 457

Document Restrictions 458

DIGITAL RIGHTS MANAGEMENT 458 • DATA EXTRUSION MANAGEMENT 458 • EXTRUSION PREVENTION 458

Data Loss Prevention Systems 459

DLP AT THE GATEWAY 460 • DLP ON CLIENTS 460 • DLP FOR DATA STORAGE 460 • DLP MANAGER 460 • WATERMARKS 460 • REMOVABLE MEDIA CONTROLS 461 • PERSPECTIVE 461

Employee Training 461

SOCIAL NETWORKING 462

Data Destruction 462

NOMINAL DELETION 462 • BASIC FILE DELETION 462 • WIPING/CLEARING 463 • DESTRUCTION 464

9.7 Conclusion 464

Security @ Work: Big Data...Losses 465

Security Technology: Geofencing for Businesses 466

Security Ethics: Paid Deletion 468

Thought Questions 469 • Hands-on Projects 469 • Project Thought Questions 470 • Case Discussion Questions 471 • Perspective Questions 472

10 Incident and Disaster Response 473

10.1 Introduction 473

Incidents Happen 473

Incident Severity 473

FALSE ALARMS 474 • MINOR INCIDENTS 474 • MAJOR INCIDENTS 474 • DISASTERS 474

Speed and Accuracy 475

SPEED IS OF THE ESSENCE 475 • SO IS ACCURACY 475 • PLANNING 475 • REHEARSAL 476

In the News 477

10.2 The Intrusion Response Process for Major Incidents 478

Detection, Analysis, and Escalation 478

DETECTION 478 • ANALYSIS 478 • ESCALATION 478

Containment 479

DISCONNECTION 479 • BLACK HOLING THE ATTACKER 480 • CONTINUING TO COLLECT DATA 480

Recovery	480	Testing and Updating the Plan	507
REPAIR DURING CONTINUING SERVER OPERATION 480 • RESTORATION FROM BACKUP TAPES 481 • TOTAL SOFTWARE REINSTALLATION 481		10.5 IT Disaster Recovery	507
Apology	481	Types of Backup Facilities	508
Punishment	482	HOT SITES 508 • COLD SITES 509 • CLOUD-BASED HOSTING 509	
PUNISHING EMPLOYEES 482 • THE DECISION TO PURSUE PROSECUTION 482 • COLLECTING AND MANAGING EVIDENCE 482		Office PCs	510
Postmortem Evaluation	484	DATA BACKUP 510 • NEW COMPUTERS 510 • WORK ENVIRONMENT 510	
Organization of the CSIRT	484	Restoration of Data and Programs	510
Legal Considerations	485	Testing the IT Disaster Recovery Plan	510
Criminal versus Civil Law	485	10.6 Conclusion	511
Jurisdictions	486	Security @ Work: Largest! Data! Breach! Ever!	511
The U.S. Federal Judicial System	486	Security Technology: Security Education and Certification	513
U.S. State and Local Laws	486	Security Ethics: Big Brother Wearables	515
International Law	487	Thought Questions 516 • Hands-on Projects 516 • Project Thought Questions 518 • Case Discussion Questions 519 • Perspective Questions 519	
Evidence and Computer Forensics	487	Module A Networking Concepts	520
U.S. Federal Cybercrime Laws	490	A.1 Introduction	520
Computer Hacking, Malware Attacks, Denial-of-Service Attacks, and Other Attacks (18 U.S.C. § 1030)	491	A.2 A Sampling of Networks	521
HACKING 491 • DENIAL-OF-SERVICE AND MALWARE ATTACKS 491 • DAMAGE THRESHOLDS 491		A Simple Home Network	521
Confidentiality in Message Transmission	492	THE ACCESS ROUTER 521 • PERSONAL COMPUTERS 521 • UTP WIRING 521 • INTERNET ACCESS LINE 522	
Other Federal Laws	492	A Building LAN	523
10.3 Intrusion Detection Systems	493	A Firm’s Wide Area Networks	524
Functions of an IDS	493	The Internet	525
LOGGING (DATA COLLECTION) 493 • AUTOMATED ANALYSIS BY THE IDS 494 • ACTIONS 494 • LOG SUMMARY REPORTS 495 • SUPPORT FOR INTERACTIVE MANUAL LOG ANALYSIS 495		Applications	528
Distributed IDSs	495	A.3 Network Protocols and Vulnerabilities	528
AGENTS 495 • MANAGER AND INTEGRATED LOG FILE 495 • BATCH VERSUS REAL-TIME DATA TRANSFER 495 • SECURE MANAGER-AGENT COMMUNICATION 496 • VENDOR COMMUNICATION 496		Inherent Security	528
Network IDSs	497	Security Explicitly Designed into the Standard	529
STAND-ALONE NIDSs 497 • SWITCH AND ROUTER NIDSs 497 • STRENGTHS OF NIDSs 497 • WEAKNESSES OF NIDSs 497 • HOST IDSs 498 • ATTRACTION OF HIDSs 498 • WEAKNESSES OF HOST IDSs 498 • HOST IDSs: OPERATING SYSTEM MONITORS 498		Security in Older Versions of the Standard	529
Log Files	499	Defective Implementation	529
TIME-STAMPED EVENTS 499 • INDIVIDUAL LOGS 499 • INTEGRATED LOGS 499 • MANUAL ANALYSIS 500		A.4 Core Layers in Layered Standards Architectures	529
Managing IDSs	501	A.5 Standards Architectures	530
TUNING FOR PRECISION 501		The TCP/IP Standards Architecture	530
Honey pots	502	The OSI Standards Architecture	531
10.4 Business Continuity Planning	503	The Hybrid TCP/IP-OSI Architecture	531
Principles of Business Continuity Management	505	A.6 Single-Network Standards	532
PEOPLE FIRST 505 • REDUCED CAPACITY IN DECISION MAKING 505 • AVOIDING RIGIDITY 505 • COMMUNICATION, COMMUNICATION, COMMUNICATION 506		The Data Link Layer	532
Business Process Analysis	506	The Physical Layer	533
IDENTIFICATION OF BUSINESS PROCESSES AND THEIR INTERRELATIONSHIPS 506 • PRIORITIZATION OF BUSINESS PROCESSES 506 • SPECIFY RESOURCE NEEDS 506 • SPECIFY ACTIONS AND SEQUENCES 506		UTP 533 • OPTICAL FIBER 533 • WIRELESS TRANSMISSION 533 • SWITCH SUPERVISORY FRAMES 533	
		A.7 Internetworking Standards	534
		A.8 The Internet Protocol	535
		The IP Version 4 Packet	535
		The First Row	535
		The Second Row	536
		The Third Row	536
		Options	537

xiv Contents

The Source and Destination IP Addresses	537	A.10 The User Datagram Protocol	547
Masks	538	A.11 TCP/IP Supervisory Standards	548
IP Version 6	538	Internet Control Message Protocol	548
IPsec	539	The Domain Name System	549
A.9 The Transmission Control Protocol	540	Dynamic Host Configuration Protocol	550
TCP: A Connection-Oriented and Reliable Protocol	540	Dynamic Routing Protocols	551
CONNECTIONLESS AND CONNECTION-ORIENTED PROTOCOLS 540 • RELIABILITY 542		Simple Network Management Protocol	552
Flag Fields	542	A.12 Application Standards	553
Sequence Number Field	543	HTTP AND HTML 554 • E-MAIL 554 • TELNET, FTP, AND SSH 554 • OTHER APPLICATION STANDARDS 554	
Acknowledgment Number Field	544	A.13 Conclusion	555
Window Field	544	Hands-on Projects 556 • Project Thought Questions 557 • Perspective Questions 557	
Options	545	Glossary	558
Port Numbers	545	Index	574
PORT NUMBERS ON SERVERS 545 • PORT NUMBERS ON CLIENTS 545 • SOCKETS 546			
TCP Security	546		

Preface

The IT security industry continues to see dramatic changes every year. Data breaches, malware, cyberattacks, and information warfare are now common news stories in the mainstream media. IT security expertise that was traditionally the domain of a few experts in large organizations is now a concern for almost everyone.

Rapid changes in the IT security industry have necessitated more frequent editions and updates of this text. This edition will be available as an etext only. This will allow us to make critical updates more frequently, and insure the content captures industry changes more accurately.

What's New in This Edition?

If you have used prior editions to this text, you will notice that almost all of the material you are familiar with remains intact. New additions to the text have been driven by requests from reviewers. More specifically, reviewers asked for a text that has a new opening case, more content about data breaches, updated news articles, new business-focused articles, new in-depth technical articles, new ethics articles, new hands-on projects, and updated statistics, standards, and laws.

In addition to these changes in content, we have tried to add supplements that make the book easier to use and more engaging for students. Below is a list of the significant changes to this edition of the text.

Opening Case—The opening case in Chapter 1 discusses the data breach at Target Corp. It looks at the size of the data breach and the mechanics of exactly how the hackers were able to steal the data. It then looks at the damage caused by the data breach including lawsuits, fines, firings of Target executives, and massive changes in the payment card industry. This case acts as an illustration of the real-world threat environment corporations face today.

Expanded Material on Data Breaches—Chapter 1 includes a new section (1.2) dedicated to looking at data breaches. New charts show a timeline and size comparison for some of the largest data breaches as well as trends for types of attacks targeting corporations. The section also discusses the costs associated with data breaches.

In the News Articles—Each chapter contains expanded and updated news articles related to chapter content. All of the brief articles have been organized into a larger “In the News” article located after the first section in each chapter. Each “In the News” article contains four to five news blurbs that reference stories that have occurred in the past two years. These articles show the

relevance of the chapter material to what is actually happening in the security industry.

Security @ Work Articles—This edition has introduced a new type of article named “Security @ Work” that focuses on the impact of information security on corporations. These 10 new articles focus more on the financial, organizational, and strategic impact of security. These articles are designed to facilitate classroom discussions that require more abstract, systems, or conceptual thinking.

Security Technology Articles—This edition has also introduced a new type of article named “Security Technology,” which focuses on more technical aspects of information security. These nine new articles dive deeper into the technical details of certain subjects. These articles are designed to allow a more in-depth analysis in some interesting topics that may be missing in more theoretical textbooks.

Security Ethics Articles—Reviewers and industry professionals have asked for more cases focused on ethical situations that workers commonly face in the security industry. They want them to be able to clearly explain why certain actions could be considered *unethical*. This edition has introduced a new type of article named “Security Ethics” that walks students through hypothetical examples of problems they may face in their future job. These 10 new articles have students examine these ethical dilemmas from the *utilitarian* and *categorical imperative* perspectives discussed in Chapter 1.

New Hands-on Projects—This edition has nine new and many updated hands-on projects that use contemporary security software. Examples of these include projects related to dynamic threat maps, Untangle, Wigle.net, Have I Been Pwned, Economic Espionage, Ghostery, and VeraCrypt. Each project relates directly to the chapter material. Students are directed to take a screenshot to show they have completed the project. Projects are designed such that each student will have a unique screenshot after completing each project. Any sharing or duplication of project deliverables will be obvious.

Updated Statistics, Standards, and Laws—This edition includes updated statistics throughout each chapter as well as discussion of new standards and laws. For example, Section 2.6 includes updated discussion on FISA, CALEA, and the USA Freedom Act. The chapter also discusses changes to GDPR, FISMA 2014, COBIT, and ISO 27000. There are also numerous updates to other standards that have changed over time. For example, in Chapter 3 there are updated discussions of hashing algorithms and digital certificate fields.

Table 1 shows a detailed list of the changes made to this edition of the text.

Table 1 Changes in the Fifth Edition

Chapter	Change	Chapter	Change	
1	New statistics and charts about attacks and costs		New Security @ Work article (Security in the Sharing Economy)	
	New Section 1.2 on data breaches		New Security Ethics article (Web Recording—Everything)	
	New introductory case study (Target Corp. data breach)		Updated ISO27002 content (Security Clause 11)	
	New discussion about ransomware		Added discussion on clear desks and clear screens (ISO 27002, 11.2.9)	
	New Security @ Work article (Equihax)		Updated chapter examples and statistics	
	New Security Ethics article (The Lure of Love Bots)		Updated section on password strength, password auditing, and common passwords in Figure 5-6	
	Updated Security Technology article (Going Phishing)		New applied Project 2 (Have I Been Pwned)	
	New In the News section (Capital One, First American, Facebook, Marriott International, and other data breaches)			
	Updated data breach statistics and charts			
	New discussion about APTs			
2	Updated Project 2 with new news sites and dynamic threat map	6	New In the News section (Capital One's Cloud, China's VPN Ban, Sketchy VPNs, Kashmir Blocked)	
	New section in 2.6 on U.S. federal surveillance laws (FISA, CALEA, and USA Freedom Act)		New Security @ Work article (Watching the Watchers)	
	New Security Technology article (Top 10 Application Vulnerabilities)		New Security Ethics article (Privacy versus Productivity: The BYOD Dilemma)	
	New Security @ Work article (Security in the Sharing Economy)		Updated Security Technology article (Tor—Onion Routing)	
	New Security Ethics article (Securing Privacy)		Added DHCP port number to list of well-known port numbers (Figure 6-9)	
	New In the News section (Snowden, Google, Border Protection, Huawei, HIPAA, and GDPR)		Updated discussion of well-known, registered, and ephemeral port numbers	
	New content on General Data Protection Regulation (GDPR)		Updated Project 2 (2018 NCSC report on Economic Espionage)	
	Updated content on data breach notification laws		7	New In the News section (Meltdown, Spectre, Foreshadow, and ZombiLoad, D-Link's Audit, and Hacked Smart Plugs)
	Updates to FISMA 2014			New Security @ Work article (Hacking Smart Things)
	Revised discussion of ROI use in security investments, oversight, promulgation, employee monitoring, and fraud detection			New Security Ethics article (MIS-Diagnosis)
Updated discussion of the USA Freedom Act	Updated Security Technology article (Antivirus Industry)			
Updated COBIT framework discussion	Updated images, and references, for Windows 10, Windows Server 2019, and Linux			
Updated ISO 27000 series discussion	Updated chapter statistics for vulnerabilities, antivirus, operating systems, etc.			
New Project 2 (Untangle®)	Updated discussion of Windows Security application, Windows Defender Firewall, mobile devices, and antitheft tracking software			
Updated Case Study to include statistics from PwC's 2018 Global State of Information Security Survey	8	New In the News section (Credential Stuffing Banks, Airbus and Boeing Software Flaws, Largest Bank Card Theft, and Bug Bounties)		
3		New Security @ Work article (Exhaustive Cheating)		
		New In the News section (No More Crypto, Encrypted Voting, WhatsApp Backdoor, Self-Encrypting SSDs, The Death of Encryption)		New Security Ethics article (Free Apps for Data)
		New Security @ Work article (Social Engineering Bitcoin)	New Security Technology article (New from Blackhat)	
		New Security Ethics article (Reverse Engineering Privacy)	New chart showing the most commonly used weak passwords	
		Updated Security Technology article (Kryptos)	New Windows 10 and IIS 10 compliant images	
		Updated discussion of hashing algorithms	Expanded discussion of SQL injection methodology including malformed SQL statements, attack methods (in-band, out-of-band, and inferential SQL injection), blind SQL injection, and preventing SQL injection (parameterization, sanitization, and using stored procedures)	
		Updated discussion of digital certificate fields	Updated statistics throughout the chapter	
		Updated chapter images and statistics	Two new projects (web browser history and Ghostery)	
		4	New In the News section (Reflected DoS Attack, DDoS for Hire, Largest DoS Attack Ever, and Hacking WPA3)	9
	New Security @ Work article (From Anthem to Anathema)		New section in 9.3 on calculating RAID 5 parity bits	
New Security Ethics article (Mining at Work)	New Security @ Work article (Big Data... Losses)			
New Security Technology article (IoT and Mirai)	New Security Ethics article (Paid Deletion)			
Updated chapter examples and statistics				
Updated Tor Project 2				
New Project 1 (Wigle.net)				
5	New In the News section (MoviePass Reset, Facebook's Biometric Lawsuit, Facial Recognition Laws, Surveillance 1984 to 2019, Forcing Your Finger)			

Chapter	Change
	New Security Technology article (Geofencing for Businesses)
	Updated discussion about SSD wiping, Blu-ray storage capacity, email retention
	New Project 1 (VeraCrypt)
10	New In the News section (Costly Climate Disasters, WikiLeaks Arrested, Evolving Honey pots)
	New Security @ Work article (Largest! Data! Breach! Ever!)
	New Security Ethics article (Big Brother Wearables)
	Updated Security Technology article (Security Education and Certifications)
	Updated Top Ten Sources of Attacks
	Discussion of cloud-based hosting in 10.5
Mod A	Updated discussion of well-known, registered, and ephemeral port numbers

Why Use This Book?

INTENDED AUDIENCE This book is written for a one-term introductory course in information security. The primary audience is upper-division BS majors in Information Systems, Computer Science, or Computer Information Systems. This book is also intended for graduate students in Masters of Information Systems (MSIS), Master of Business Administration (MBA), Master of Accountancy (MAcc), or other MS programs that are seeking a broader knowledge of information security.

It is designed to provide students with information security knowledge as it relates to corporate security. It will give students going into the information security field a solid foundation. It can also serve as a network security text.

PREREQUISITES This book can be used by students who have taken an introductory course in information systems. However, taking a networking course before using this book is strongly advisable. For students who have not taken a networking course, Module A is a review of networking with a special focus on security aspects of network concepts.

Even if networking is a prerequisite or corequisite at your school, we recommend covering Module A. It helps refresh and reinforce networking concepts.

BALANCING TECHNICAL AND MANAGERIAL CONTENT Our students are going to need jobs. When you ask working IT security professionals what they are looking for in a new hire, they give similar responses. They want proactive workers who can take initiative, learn on their own, have strong technical skills, and have a business focus.

A business focus does not mean a purely managerial focus. Companies want a strong understanding of security management. But they also want a really solid understanding of defensive security technology. A common complaint is that students who have taken managerial courses don't even know how stateful packet inspection firewalls operate, or what other types of firewalls are available. "We aren't

hiring these kids as security managers" is a common comment. This is usually followed by "They need to start as worker bees, and worker bees start with technology."

Overall, we have attempted to provide a strong managerial focus along with a solid technical understanding of security tools. Most of this book deals with the technical aspects of protective countermeasures. But even the countermeasure chapters reflect what students need to know to manage these technologies. You can "throttle" the amount of technical content by using or not using the Hands-on Projects at the end of each chapter.

How Is This Book Organized?

The book starts by looking at the threat environment facing corporations today. This gets the students' attention levels up, and introduces terminology that will be used throughout the rest of the book. Discussing the threat environment demonstrates the need for the defenses mentioned in later chapters.

The rest of the book follows the good old plan-protect-respond cycle. Chapter 2 deals with planning, and Chapter 10 deals with incident and disaster response. All of the chapters in the middle deal with countermeasures designed to protect information systems.

The countermeasures section starts with a chapter on cryptography because cryptographic protections are part of many other countermeasures. Subsequent chapters introduce secure networks, access control, firewalls, host hardening, application security, and data protection. In general, the book follows the flow of data from networks, through firewalls, and eventually to hosts to be processed and stored.

USING THE BOOK IN CLASS Chapters in this book are designed to be covered in a semester week. This leaves a few classes for exams, presentations, guest speakers, hands-on activities, or material in the module. Starting each class with a demonstration of one of the hands-on projects is a good way to get students' attention.

It's important for students to read each chapter before it's covered in class. The chapters contain technical and conceptual material that needs to be closely studied. We recommend either giving a short reading quiz or requiring students to turn in Test Your Understanding questions before covering each chapter.

SECURITY @ WORK, TECHNOLOGY, AND ETHICS ARTICLES These articles are included to facilitate classroom discussions, in-class small group breakouts, or additionally assigned homework. Some instructors want to offer an information security class with an *organizational* focus, while others want a more *technical* focus. These articles are designed to allow instructors to adapt the text to their teaching goals. The ethics articles were recommended as a key component because more schools are integrating

ethics across all classes in their curriculum. Some are including ethics modules as part of AACSB accreditation, and others just want to be sure an ethical component is included in their information security course.

POWERPOINT SLIDES AND STUDY FIGURES The PowerPoint lectures cover nearly everything, as do the study figures in the book. Study figures even summarize main points from the text. This makes the PowerPoint presentations and the figures in the book great study aids.

TEST YOUR UNDERSTANDING QUESTIONS After each section or subsection, there are Test Your Understanding questions. This lets students check if they really understood what they just read. If not, they can go back and master that small chunk of material before going on. The test item file questions are linked to particular Test Your Understanding questions. If you cut some material out, it is easy to know what multiple-choice questions not to use.

INTEGRATIVE THOUGHT QUESTIONS At the end of each chapter, there are integrative Thought Questions, which require students to synthesize what they have learned. They are more general in nature and require the application of the chapter material beyond rote memorization.

HANDS-ON PROJECTS Students often comment that their favorite part of the course is the Hands-on Projects. Students like the Hands-on Projects because they get to use contemporary information security software that relates to the chapter material. Each chapter has at least two applied projects and subsequent Project Thought Questions.

Each project requires students to take a unique screenshot at the end of the project as proof they completed the project. Each student's screenshot will include a time stamp, the student's name, or another unique identifier.

CASE STUDY Each chapter includes a real-world case study focused on how information security affects corporations. More specifically, each case study is designed to illustrate how the material presented in the chapter could impact a corporation. Along with each case study are related key findings from prominent annual industry reports. Links to each industry report are provided and can be used as supplementary reading. Case studies, combined with key findings from relevant industry reports, should provide ample material for classroom discussion.

CASE DISCUSSION QUESTIONS Case studies are followed by a series of open-ended questions to guide case-based classroom discussions. They offer students the opportunity to apply, analyze, and synthesize the material presented in the chapter within the context of a real-world business case.

PERSPECTIVE QUESTIONS There are two general questions that ask students to reflect on what they have studied. These questions give students a chance to think comprehensively about the chapter material at a higher level.

HEY! WHERE'S ALL THE ATTACK SOFTWARE? This book does not teach students how to break into computers. There is software designed specifically to exploit vulnerabilities and gain access to systems. This book does not cover this type of software. Rather, the focus of the book is how to proactively defend corporate systems from attacks.

Effectively securing corporate information systems is a complicated process. Learning how to secure corporate information systems requires the entire book. Once students have a good understanding of how to secure corporate systems, they *might* be ready to look at penetration testing software.

With 10 chapters, you do have time to introduce some offense. However, if you do teach offense, do it carefully. Attack tools are addictive, and students are rarely satisfied using them in small labs that are carefully air-gapped from the broader school network and the Internet. A few publicized attacks by your students can get IT security barred from the curriculum.

Instructor Supplements

This is a hard course to teach. We have tried to build in as much teacher support as possible. Our goal was to reduce the total amount of preparation time instructors had to spend getting ready to teach this course.

Learning new course material, monitoring current events, and managing an active research agenda is time-consuming. We hope the instructor supplements make it easier to teach a high-quality course with less prep time.

ONLINE INSTRUCTOR RESOURCES The Pearson Higher Education website (<http://www.pearsonhighered.com>) has all of the supplements discussed below. These include the PowerPoint lectures, test item file, TestGen software, teacher's manual, and a sample syllabus.

POWERPOINT LECTURES There is a PowerPoint lecture for each chapter. They aren't "a few selected slides." They are full lectures with detailed figures and explanations. And they aren't made from figures that look pretty in the book but that are invisible on slides. We have tried to create the PowerPoint slides to be pretty self-explanatory.

TEST ITEM FILE The test item file for this book makes creating, or supplementing, an exam with challenging multiple-choice questions easy. Questions in the test item file refer directly to the Test Your Understanding questions located throughout each chapter. This means exams will be tied directly to concepts discussed in the chapter.

TEACHER'S MANUAL The Teacher's Manual has suggestions on how to teach the chapters. For instance, the book begins with threats. In the first class, you could have students list everybody who might attack them. Then have them come up with *ways* each group is likely to attack them. Along the way, the class discussion naturally can touch on chapter concepts such as the distinction between viruses and worms.

SAMPLE SYLLABUS We have included a sample syllabus if you are teaching this course for the first time. It can serve as a guide to structuring the course and reduce your prep time.

STUDENT FILES Study Guide and Homework files in Word are available for download by accessing www.pearsonhighered.com/boyle.

E-MAIL US Please feel free to e-mail us. You can reach Randy at RandyBoyle@Weber.edu, or Ray at Ray@Panko.com. Your Pearson Sales Representative can provide you with support, but if you have a question, please also feel free to contact us. We'd also love suggestions for the next edition of the book and for additional support for this edition.

We would also like to thank the industry experts who contributed to this edition. Their expertise and perspective added a real-world perspective that can only come from years of practical experience. Thanks to Dr. Jeffrey Proudfoot, Matt Christensen, Dan McDonald, Amber Schroader, Chris Larsen, David Glod, Andrew Yenchik, Stephen Burton, Susan Jensen, and Bruce Wignall.

Thanks also go to our former, and now happily retired, editor Bob Horan for his years of friendship, support, and wise counsel. Finally, like so many authors in college publishing, we owe tremendous thanks to our current editors, Allie D'Aprile and Jenifer Niles. Allie and Jenifer continue to provide us with the skilled guidance necessary to make this text a great success.

Special thanks go to the production team that actually makes the book. Most readers won't fully appreciate the hard work and dedication it takes to transform the "raw" content provided by authors into the finished copy you're reading now. The commitment and attention detail from Pearson's production team have made this into a great book. We also want to thank the tireless sales force that plays a key role in getting students the best educational materials possible. Their professionalism and hard work make a difference.

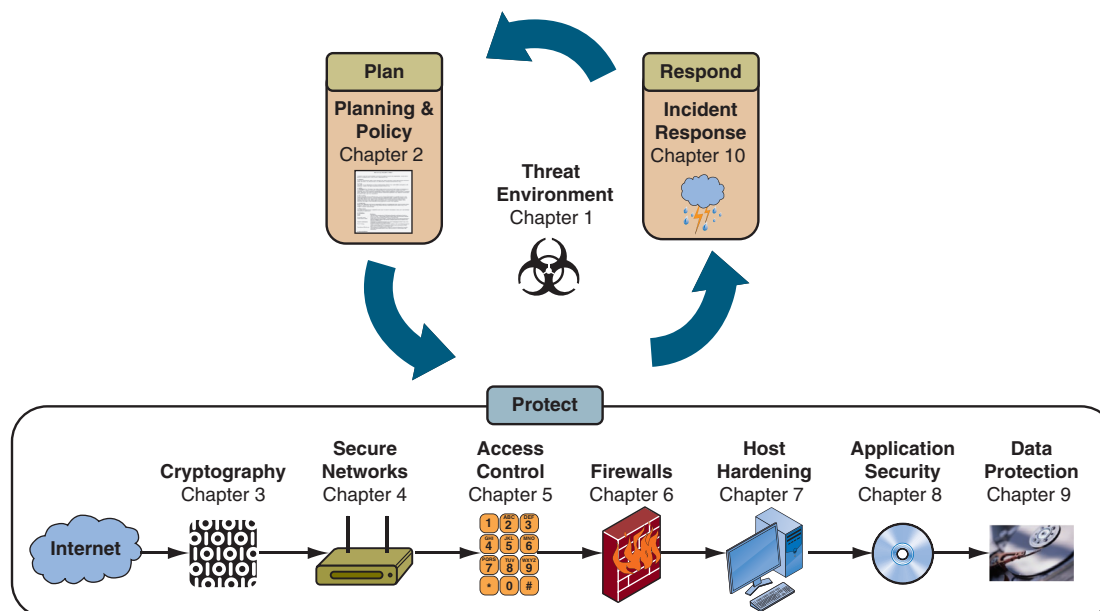
Lastly, and most importantly, I (Randy) would like to thank Ray. Like many of you, I have used Ray's books for years. Ray has a writing style that students find accessible and intuitive. Ray's books are popular and widely adopted by instructors across the country. His books have been the source of networking and security knowledge for many workers currently in the industry.

I'm grateful that Ray trusted me enough to work on one of his books. I hope this edition continues in the legacy of great texts Ray has produced. It's an honor to work with a generous person like Ray.

*Randy Boyle
Ray Panko*

Acknowledgments

We would like to thank all of the reviewers of prior editions, and more specifically the reviewers of the current edition, including Adrian Brown, Li-Chiou Chen, Jae J. Choi, Raymond Curts, Ahmad Ghafarian, Sushma Mishra, Mark Pisano, Rassul Saeedipour, Brenda Wamsley, and Ping Wang. They have used this book for years and know it well. Their suggestions, recommendations, and criticisms helped shape this edition. This book really is a product of a much larger community of academics and researchers.



About the Authors



Randall J. Boyle is an associate professor of Management Information Systems and Willard Eccles Fellow at Weber State University in the Goddard School of Business and Economics. He received his PhD in Management Information Systems from Florida State University in 2003. He also has a master's degree in Public Administration and a BS in Finance. His research areas include deception detection in computer-mediated environments, data breaches, secure information systems, the effects of IT on cognitive biases, and the effects of IT on knowledge workers. He has received college teaching awards at Weber State University, Longwood University, the University of Utah, and the University of Alabama in Huntsville. His teaching is primarily focused on management information systems, information security, and networking. He has authored several books including *Using MIS 11e*, *Experiencing MIS 9e*, *Corporate Computer Security 5e*, *Applied Information Security*, and *Applied Networking Labs*.



Ray Panko is Professor Emeritus of Information Technology Management at the University of Hawai'i's Shidler College of Business. His main courses are networking and security. Before coming to the university, he was a project manager at Stanford Research Institute (now SRI International), where he worked for Doug Englebart (the inventor of the mouse). He received his BS in Physics and his MBA from Seattle University. He received his doctorate from Stanford University, where his dissertation was conducted under contract to the Office of the President of the United States. He has been awarded the Shidler College of Business's Dennis Ching award as the outstanding teacher among senior faculty. He is also a Shidler Fellow.