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

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://lccn.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

Contents

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

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 Honeypots)
	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.

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.

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.

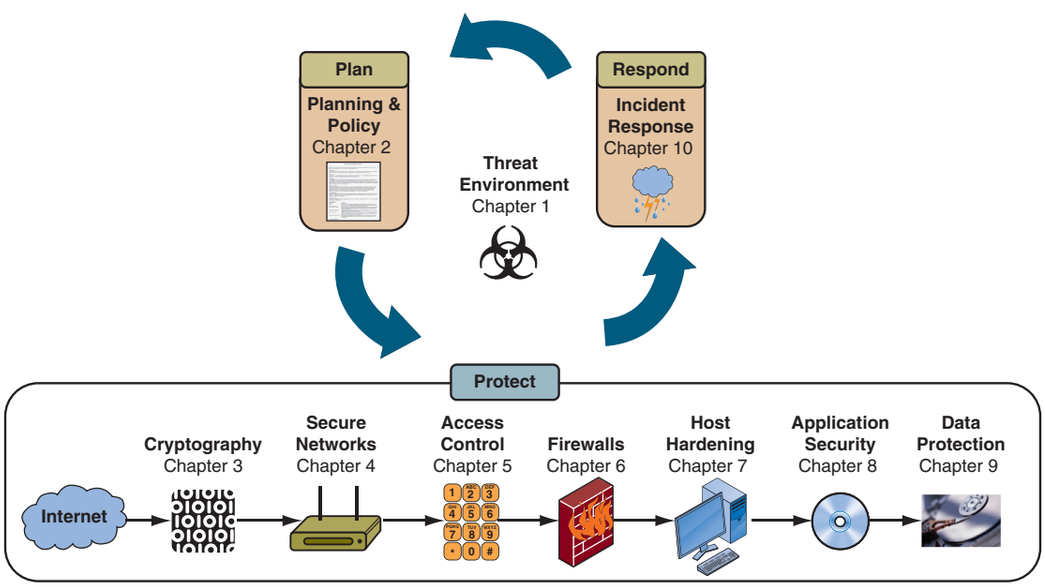
Thanks also go to our former, and now happily retired, editor Bob Horan for his years of friendship, support, and wise counsel. Finally, like so many authors in college publishing, we owe tremendous thanks to our current editors, Allie D'Aprile and Jenifer Niles. Allie and Jenifer continue to provide 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



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.