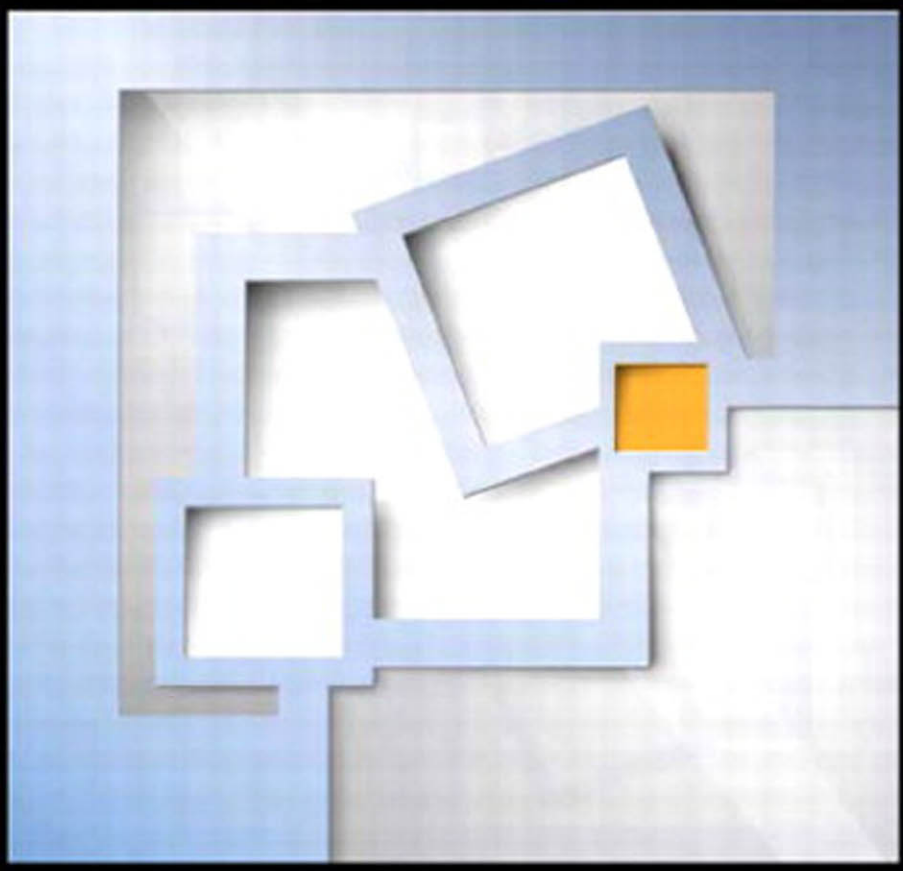


CORPORATE COMPUTER SECURITY

FOURTH EDITION

Randall J. Boyle | Raymond R. Panko

OTHER MIS TITLES OF INTEREST

INTRODUCTORY MIS:

Managing Information Technology, 7/e
Brown, DeHayes, Hoffer, Martin & Perkins ©2012

SharePoint for Students
Cole, Fox & Kroenke ©2012

Experiencing MIS, 5/e
Kroenke ©2015

Using MIS, 7/e
Kroenke ©2015

MIS Essentials, 4/e
Kroenke ©2015

Management Information Systems, 13/e
Laudon & Laudon ©2014

Essentials of Management Information

Systems, 11/e
Laudon & Laudon ©2015

IT Strategy, 3/e
McKeen & Smith ©2015

Processes, Systems, and Information: An Introduction to MIS, 2/e
McKinney & Kroenke ©2015

Essentials of Processes, Systems and Information: With SAP Tutorials
McKinney & Kroenke ©2014

Information Systems Today, 6/e
Valacich & Schneider ©2014

Introduction to Information Systems, 2/e
Wallace ©2015

DATABASE:

Hands-on Database, 2/e
Conger ©2014

Modern Database Management, 11/e
Hoffer, Ramesh & Topi ©2013

Database Systems: Introduction to Databases and Data Warehouses
Jukic, Vrbsky & Nestorov ©2014

Essentials of Database Management
Hoffer, Topi & Ramesh ©2014

Database Concepts, 7/e
Kroenke & Auer ©2015

Database Processing, 13/e
Kroenke & Auer ©2014

SYSTEMS ANALYSIS AND DESIGN:

Modern Systems Analysis and Design, 7/e
Hoffer, George & Valacich ©2014

Systems Analysis and Design, 9/e
Kendall & Kendall ©2014

Essentials of Systems Analysis and Design, 6/e
Valacich, George & Hoffer ©2015

DECISION SUPPORT SYSTEMS:

Business Intelligence, 3/e
Sharda, Delen & Turban ©2014

Decision Support and Business Intelligence Systems, 10/e
Sharda, Delen & Turban ©2014

DATA COMMUNICATIONS & NETWORKING:

Applied Networking Labs, 2/e
Boyle ©2014

Digital Business Networks
Dooley ©2014

Business Driven Data Communications
Gendron ©2013

Business Data Networks and Security, 10/e
Panko & Panko ©2015

ELECTRONIC COMMERCE:

E-Commerce: Business, Technology, Society, 11/e
Laudon & Traver ©2015

E-Commerce Essentials
Laudon & Traver ©2014

Electronic Commerce 2012
Turban, King, Lee, Liang & Turban ©2012

ENTERPRISE RESOURCE PLANNING:

Enterprise Systems for Management, 2/e
Motiwalla & Thompson ©2012

PROJECT MANAGEMENT:

Project Management: Process, Technology and Practice
Vaidyanathan ©2013

SECURITY:

Applied Information Security, 2/e
Boyle ©2014

Corporate Computer Security, 3/e
Boyle & Panko ©2013

Fourth Edition

Corporate Computer Security

Randall J. Boyle
Longwood University

Raymond R. Panko
University of Hawai`i at Mānoa

PEARSON

Boston Columbus Indianapolis New York San Francisco Upper Saddle River
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montréal Toronto
Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

To Courtney Boyle, thank you for your patience, kindness, and perspective on what's most important in life.

—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

Editor in Chief: Stephanie Wall
Executive Editor: Bob Horan
Program Manager Team Lead: Ashley Santora
Program Manager: Denise Vaughn
Director of Marketing: Maggie Moylan
Executive Marketing Manager: Anne Fahlgren
Project Manager Team Lead: Judy Leale
Project Manager: Tom Benfatti
Operations Specialist: Michelle Klein
Creative Director: Jayne Conte
Cover Designer: Bruce Kenselaar
Digital Production Project Manager: Lisa Rinaldi
Full-Service Project Management: Prabhu Chinnasamy, Integra Software Services Pvt. Ltd.
Printer/Binder: Courier/Westford
Cover Printer: Lehigh-Phoenix
Text Font: Times, 10/12

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

Library of Congress Cataloging-in-Publication Data on File

10 9 8 7 6 5 4 3 2 1

PEARSON

ISBN 10: 0-13-354519-9
ISBN 13: 978-0-13-354519-7

CONTENTS

PREFACE

The IT security industry has seen dramatic changes in the past decades. Security breaches, data theft, cyber attacks, 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 has now become a concern for almost everyone.

These rapid changes in the IT security industry have necessitated more recent editions of this text. Old attacks are being used in new ways, and new attacks are becoming commonplace. We hope the changes to this new edition have captured some of these changes in the industry.

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, business case studies at the end of each chapter, new hands-on projects, updated news articles, and more information related to certifications.

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 covers a series of data breaches that resulted in one of the largest known data losses to date. The case looks at the sequence of events surrounding the three data breaches at Sony Corp. It then examines how the attackers were able to steal the data, possible motives behind the attacks, arrests and punishment of the attackers, and the impacts on Sony Corp. This case acts as an illustration of the real-world threat environment corporations face today.

Business Case Studies—This edition has tried to have more of a business focus by adding in a real-world case study at the end of each chapter. The case studies are designed to show how the material presented in the chapter could have a direct impact on an actual corporation. After each case study, there are key findings from prominent annual industry reports related to the case and chapter material. Case studies, combined with key findings from relevant industry reports, should provide ample material for classroom discussion. Open-ended case questions are included to help guide case discussions. They also offer students the opportunity to apply, analyze, and synthesize the material presented in the chapter.

New Hands-on Projects—Each chapter has new, or updated, hands-on projects that use contemporary security software. 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 News Articles—Each chapter contains expanded and updated IT security news articles. Over 80 percent of the news articles in this book reference stories that have occurred since the prior edition was published.

Expanded Material on Certifications—Reviewers of the prior edition asked for more material related to IT security certifications. We live in a world that relies on credentials as a means of conveying legitimacy, skill, and possibly experience. In this respect, the security field is no different. To this end, we have updated and expanded the certification focus article in Chapter 10. It is likely that students pursuing a career in the IT security industry will seek some type of certification.

Why Use This Book?

INTENDED AUDIENCE This book is written for a one-term introductory course in IT 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 IT security.

It is designed to provide students with IT security knowledge as it relates to corporate security. It will give students going into the IT 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.

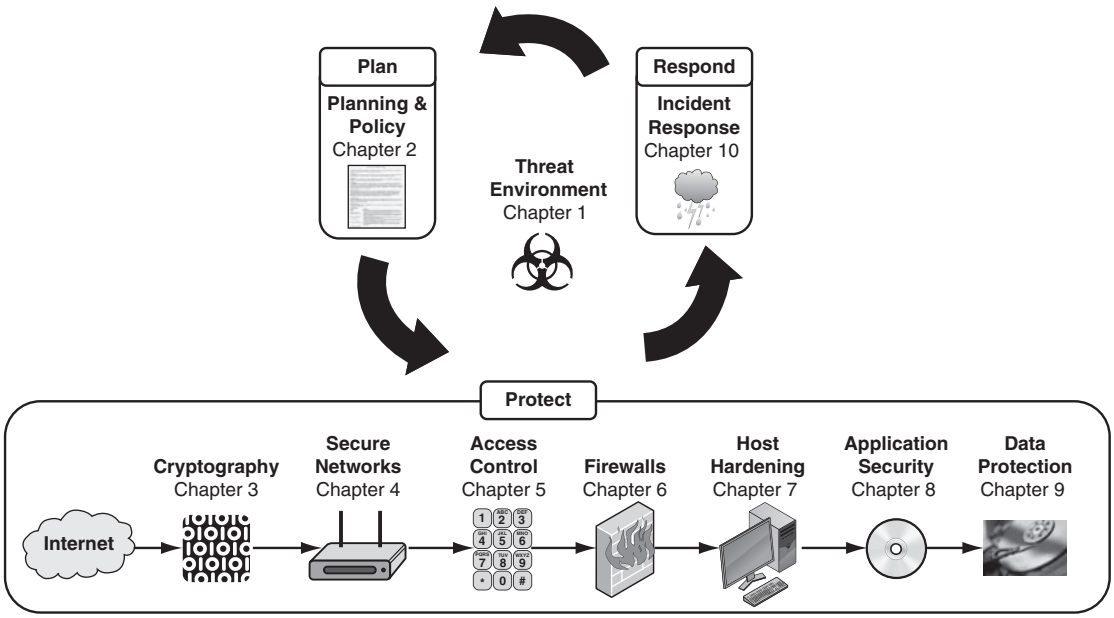
BALANCING TECHNICAL AND MANAGERIAL CONTENT Our students are going to need jobs. When you ask working IT security professionals what they are looking for in a new hire, they give similar responses. They want proactive workers who can take initiative, learn on their own, have strong technical skills, and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

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 IT 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 IT 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 BoyleRJ@Longwood.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. 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 Matt Christensen, Dan McDonald at Utah Valley University, Amber Schroader at Paraben Corp., Chris Larsen at BlueCoat Systems, Inc., David Glod at Grant Thornton, Andrew Yenchik, Stephen Burton, and Susan Jensen at Digital Ranch, Inc., Morpho, and Bruce Wignall at Teleperformance Group.

We thank our editor Bob Horan for his support and guidance. A good editor can produce good books. Bob is a great editor who produces great books. And he has done so for many years. We feel privileged to be able to work with Bob.

Special thanks go to Denise Vaughn, Karin Williams, Ashley Santora, and 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 holding in your hands. Denise, Karin, Ashley, and the Pearson production team's commitment and attention to detail have made this into a great book.

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

Randy Boyle is a professor at the College of Business and Economics at Longwood University. He received his PhD in Management Information Systems (MIS) 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, information assurance policy, the effects of IT on cognitive biases, and the effects of IT on knowledge workers. He has received college teaching awards at the University of Alabama in Huntsville, the University of Utah, and Longwood University. His teaching is primarily focused on information security, networking, and management information systems. He is the author of *Applied Information Security* and *Applied Networking Labs*.

Ray Panko is a professor of IT 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.

This page intentionally left blank

CHAPTER 1

The Threat Environment

Chapter Outline

Learning Objectives

After studying this chapter, you should be able to:

- Define the term *threat environment*.
- Use basic *security terminology*.
- Describe threats from *employees* and ex-employees.
- Describe threats from *malware* writers.
- Describe traditional external hackers and their *attacks*, including break-in processes, social engineering, and denial-of-service attacks.
- Know that *criminals* have become the dominant attackers today, describe the types of attacks they make, and discuss their methods of cooperation.
- Distinguish between *cyberwar* and *cyberterror*.

1.1 INTRODUCTION

The world today is a dangerous place for corporations. The Internet has given firms access to billions of customers and other business partners, but it has also given criminals access to hundreds of millions of corporations and individuals. Criminals are able to attack websites, databases, and critical information systems without ever entering the corporation's host country.

Corporations have become critically dependent on information technology (IT) as part of their overall competitive advantage. In order to protect their IT infrastructure from a variety of threats, and subsequent profitability, corporations must have comprehensive IT security policies, well-established procedures, hardened applications, and secure hardware.

Basic Security Terminology

THE THREAT ENVIRONMENT If companies are to be able to defend themselves, they need an understanding of the **threat environment**—that is, the types of attackers and attacks companies face. "Understanding the threat environment" is a fancy way of saying "Know your enemy." If you do not know how you may be attacked, you cannot plan to defend yourself. This chapter will focus almost exclusively on the threat environment.

The threat environment consists of the types of attackers and attacks that companies face.

The Threat Environment
The threat environment consists of the types of attackers and attacks that companies face

Security Goals
Confidentiality
Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network

Integrity
Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data

Availability
Availability means that people who are authorized to use information are not prevented from doing so

Compromises
Successful attacks
Also called incidents and breaches

Countermeasures
Tools used to thwart attacks
Also called safeguards, protections, and controls
Types of countermeasures
Preventative
Detective
Corrective

FIGURE 1-1 Basic Security Terminology (Study Figure)

SECURITY GOALS Corporations and subgroups in corporations have **security goals**—conditions that the security staff wishes to achieve. Three common core goals are referred to collectively as **CIA**. This is not the Central Intelligence Agency. Rather, CIA stands for confidentiality, integrity, and availability.

- ***Confidentiality***—Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.
- ***Integrity***—Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.
- ***Availability***—Availability means that people who are authorized to use information are not prevented from doing so. Neither a computer attack nor a network attack will keep them away from the information they are authorized to access.

Many security specialists are unhappy with the simplistic CIA goal taxonomy because they feel that companies have many other security goals. However, the CIA goals are a good place to begin thinking about security goals.

COMPROMISES When a threat succeeds in causing harm to a business, this is called an **incident**, **breach**, or **compromise**. Companies try to deter incidents, of course, but they usually have to face several breaches each year, so response to incidents is a critical skill. In terms of the business process model, threats push the business process away from meeting one or more of its goals.

When a threat succeeds in causing harm to a business, this is called an incident, breach, or compromise.

COUNTERMEASURES Naturally, security professionals try to stop threats. The methods they use to thwart attacks are called **countermeasures**, **safeguards**, **protections**, or **controls**. The goal of countermeasures is to keep business processes on track for meeting their business goals despite the presence of threats and actual compromises.

Tools used to thwart attacks are called countermeasures, safeguards, or controls.

Countermeasures can be technical, human, or (most commonly) a mixture of the two. Typically, countermeasures are classified into three types:

- ***Preventative***—Preventative countermeasures keep attacks from succeeding. Most controls are preventative controls.
- ***Detective***—Detective countermeasures identify when a threat is attacking and especially when it is succeeding. Fast detection can minimize damage.
- ***Corrective***—Corrective countermeasures get the business process back on track after a compromise. The faster the business process can get back on track, the more likely the business process will be to meet its goals.

TEST YOUR UNDERSTANDING

1. **a.** Why is it important for firms to understand the threat environment?
   b. Name the three common security goals.
   c. Briefly explain each goal.
   d. What is an incident?

e. What are the synonyms for *incidents*?
f. What are countermeasures?
g. What are the synonyms for *countermeasure*?
h. What is the goal of countermeasures?
i. What are the three types of countermeasures?

CASE STUDY

The Sony Data Breaches

If this terminology seems abstract, it may help to look at a specific attack to put these terms into context and to show how complex security attacks can be. We will begin with one of the largest losses of private customer information. These were a series of data breaches at Sony Corporation.

Sony Corporation

Sony Corporation is a Japanese multinational corporation founded in 1946 that focuses on electronics, game, entertainment, and financial services. It employs about 146,300 people and has annual revenues of about $72.3 billion. Sony is widely known for its televisions, digital imaging, audio/video hardware, PCs, semiconductors, electronic components, and gaming platform.

The First Attack

The first of three attacks on Sony occurred on April 17–19, 2011, just weeks after the catastrophic earthquake, tsunami, and subsequent reactor meltdowns in Japan. Attackers used SQL injection to steal 77 million accounts containing personally identifiable information (PII) including names, addresses, dates of birth, usernames, passwords, security questions, and some credit card numbers.[1] Considering the amount and sensitive nature of the data stolen, this attack is easily one of the most severe losses of consumer data to date.

Sony detected unusual server activity on April 19 and brought in forensic examiners to determine if data may have been stolen.[2] On April 20, Sony turned off access to the entire 77 million-user Sony PlayStation Network (PSN) fearing that the attackers accessed user accounts. Sony then provided the FBI with information about the attack.

Sony publicly acknowledged the intrusion on April 26, more than a week after it became aware of it. Sony would later face scrutiny about its decision to delay telling its customers that attackers had access to their account information for a full week.

On April 30, the CEO of Sony, Kazuo Hirai, apologized to PSN gamers for the loss of their account information and the continuing PSN outage.[3] At the press conference Hirai said,

> These illegal attacks obviously highlight the widespread problem with cybersecurity. We take the security of our consumers' information very seriously and are committed to helping our consumers protect their personal data. In addition,

[1] Shane Richmond and Christopher Williams. "Millions of Internet Users Hit by Massive Sony PlayStation Data Theft," *The Telegraph*, April 26, 2011. http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html.
[2] Dean Takahashi, "Chronology of the Attack on Sony's PlayStation Network," *VentureBeat.com*, May 4, 2011. http://venturebeat.com/2011/05/04/chronology-of-the-attack-on-sonys-playstation-network/#QuSrgtEootxXhtil.99.
[3] Dean Takahashi, "Sony Executive Kaz Hirai Apologizes for PlayStation Network Outage," *VentureBeat.com*, April 30, 2011. http://venturebeat.com/2011/04/30/psn-outage-apolog/.

Sony Corporation

Multinational corporation focused on electronics, game, entertainment, and financial services

Has approximately 146,300 employees and $72.3 billion in revenue

The First Attack

Occurred weeks after a catastrophic earthquake, tsunami, and subsequent reactor meltdowns in Japan

SQL injection was used to steal 77 million accounts with personally identifiable information

PlayStation Network shutdown for weeks

More than a week delay in notifying users about the data loss

Increased level of security

The Second Attack

Additional 24.6 million accounts stolen from Sony Online Entertainment

Similar SQL injection attack

Greatly enhanced security put in place

PlayStation Network offline for about three weeks

The Third Attack

One million additional user accounts stolen from SonyPictures.com

Weeks after PlayStation Network comes back online

LulzSec takes credit

Attackers claim to have used a simple SQL injection technique

The Attack Method—SQL Injection

Sending modified SQL statements through web application

Unexpected values passed

Attempts to alter how SQL statement is processed

Can be used to manipulate stored data

Attackers and Their Motives

Members of LulzSec and Anonymous

Possibly motivated by Sony's lawsuit against George Hotz for jailbreaking PlayStation 3

Multiple arrests, convictions, prison sentences, and fines

Informant help identify other attackers

The Fallout

Sony provided free identity theft services and online games

£250,000 fine from the UK

Estimated losses at $171 million

FIGURE 1-2 The Sony Data Breaches (Study Figure)

(*continued*)

the organization has worked around the clock to bring these services back online, and are doing so only after we had verified increased levels of security across our networks.

The Second Attack

The ink wasn't dry from the humbling press conference when Sony found evidence of a new attack on May 1.[4] On May 2, forensic investigators found evidence that an *additional* 24.6 million user accounts were compromised in a similar SQL injection attack on Sony Online Entertainment. In addition to the user account information, more than 12,700 credit card numbers and 10,700 debit card numbers had been stolen. Sony later clarified that only 900 of the possible 12,700 credit card numbers were still active.[5]

All of Sony Online Entertainment servers were immediately taken down. The total number of lost accounts was now over 100 million. Hundreds of servers were shut down, gaming services were unavailable for millions of users, and future compensation costs were mounting.

On May 4, Kazuo Hirai submitted a written response to the U.S. Congress about the attacks.[6] He specifically mentioned the steps that Sony was taking to prevent future breaches including enhanced "data protection and encryption enhanced ability to detect software intrusions, unauthorized access and unusual activity patterns; additional firewalls; establishment of a new data center in an undisclosed location with increased security; and the naming of a new Chief Information Security Officer."

On May 15, some PSN services started coming online in select countries after being offline for about three weeks. Sony estimated that the costs related to the attacks would be over $171 million.[7] According to Sony, credit card companies had not reported any fraudulent transactions associated with the intrusion.

The Third Attack

Sony was besieged by yet another online SQL injection attack only a few weeks after PSN services started coming back online.[8] On June 2, a group named LulzSec posted a press release and multiple data files, claiming to have stolen over 1 million user accounts from SonyPictures.com.[9] The following is part of the LulzSec press release:

> Greetings folks. We're LulzSec, and welto Sownage. Enclosed you will find various collections of data stolen from internal Sony networks and websites, all of which we accessed easily and without the need for outside support or money.
>
> We recently broke into SonyPictures.com and compromised over 1,000,000 users' personal information, including passwords, e-mail addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts. Among other things, we also compromised all admin

[4] Jason Schreier, "Sony Hacked Again; 25 Million Entertainment Users' Info at Risk," Wired.com, May 2, 2011. http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack/.
[5] Dan Pearson, "24.6 Million SOE Accounts Potentially Compromised," *GameIndustry.biz*, May 3, 2011. http://www.gamesindustry.biz/articles/2011-05-03-24-6-million-soe-accounts-potentially-compromised.
[6] Patrick Seybold, "Sony's Response to the U.S. House of Representatives," *PlayStation.com*, May 4, 2011. http://blog.us.playstation.com/2011/05/04/sonys-response-to-the-u-s-house-of-representatives/.
[7] Mark Hachman, "Play Station Hack to Cost Sony $171M; Quake Costs far Higher," *PCMag.com*, May 23, 2011. http://www.pcmag.com/article2/0,2817,2385790,00.asp.
[8] Christina Warren, "Sony Pictures Website Hacked, 1 Million Accounts Exposed," *Mashable.com*, June 2, 2011. http://mashable.com/2011/06/02/sony-pictures-hacked/.
[9] Julianne Pepitone, "Group Claims Fresh Hack of 1 Million Sony Accounts," *CNN Money*, June 2, 2011. http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/index.htm.

details of Sony Pictures (including passwords) along with 75,000 "music codes" and 3.5 million "music coupons."[10]

The press release went on to give more details about the attack and the contents of the associated data files. The attackers used a simple SQL injection technique to extract the stolen information. They were also critical of Sony's security efforts.

What's worse is that every bit of data we took wasn't encrypted. Sony stored over 1,000,000 passwords of its customers in plaintext, which means it's just a matter of taking it. This is disgraceful and insecure: they were asking for it.

The Attack Method—SQL Injection

What is SQL injection? SQL injection is an attack that involves sending modified SQL statements to a web application that will, in turn, modify a database. Attackers can send unexpected input through their web browser that will enable them to read from, write to, and even delete entire databases. SQL injection can even be used to execute commands on the server. SQL injection is a common attack method for many of the high-profile attacks seen in the news.

Below is a simple example of how SQL injection could be used.

****Warning***SQL injection can cause tremendous damage and harm. It is illegal to do on other systems and you will be prosecuted. Do not use SQL injection on any system without permission.*

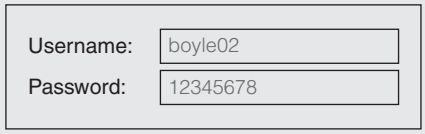


FIGURE 1-3 Normal Login

Normal SQL Statement for Login

Login screens require users to enter a username and password. These values are then passed to the web application and checked against values in the database. The SQL statement below shows how these parameters might be passed to a database for a legitimate login.

Information from this login is used to make the following SQL statement:

```
SELECT FROM Users WHERE
username='boyle02' AND
password='12345678';
```

Both the username (boyle02) and password (12345678) are strings that can include letters, numbers, and characters. They are both enclosed by single quotes, and the SQL statement ends with a semicolon.

Malformed SQL Statement for Login

In the SQL statement below, the password (12345678) is replaced with text (whatever' or 1=1—). This will alter how the SQL query is interpreted. Note that the additional single quote after the word "whatever" encloses the password. Since the actual password

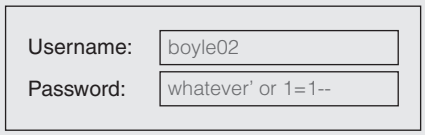


FIGURE 1-4 SQL Injection

(*continued*)

[10] The original press release was posted on http://lulzsecurity.com/. At the time of this writing, all content from the site had been removed.

(12345678) is not "whatever" the login should fail. However, the additional parameters will ensure that the login succeeds.

The rest of the injected SQL statement is processed normally. The logical operator "or" is used to create a two-part WHERE clause. The first part of the clause will return a false value for the WHERE clause. The second part of the clause, 1=1, will *always* return a *true* value. This *guarantees* that the login will succeed.

Information from this login is used to make the following malformed SQL statement:

```
SELECT FROM Users WHERE
username='boyle02' AND
password='whatever' or 1=1--';
```

In this case, SQL injection was used as a simple authentication bypass. In the case of the Sony data breaches, SQL injection was used to extract information from corporate databases through a web interface. SQL injection is covered in greater depth in Chapter 8.

Attackers and Their Motives

Members of two affiliated hacking groups, Anonymous and LulzSec, were likely behind the attacks on Sony. The Anonymous hacking group released a press statement denying involvement after Sony claimed to have found a file named "Anonymous" containing the text "We are Legion" after the first two attacks.[11]

Just before the Sony attacks, Anonymous said it was launching operation "#OpSony" in response to Sony's lawsuit against George Hotz.[12] Sony was suing George Hotz for jailbreaking its PlayStation 3. In a statement from Anonymous it said Sony would "experience the wrath of Anonymous."[13]

While LulzSec took credit for the third attack, on SonyPictures.com,[14] it's likely that the attackers were members of both groups. Numerous members of Anonymous and LulzSec were arrested for a variety of computer crimes. One such arrest occurred on September 22, 2011, when the FBI arrested Arizona native Cody Andrew Kretsinger.[15]

Kretsinger, AKA "recursion," pled guilty and was sentenced to one year and one day in federal prison after being convicted of federal computer hacking charges related to his involvement in the Sony attacks.[16] He was also ordered to perform 1,000 hours of community service and pay $605,663 in restitution.

Another LulzSec member, Hector Monsegur, AKA "Sabu," was awaiting sentencing at the time of this writing. Monsegur faces a possible 122 years in prison for various computer crimes. Federal investigators will likely recommend a greatly reduced sentence because he was the key informant who helped identify numerous other members of LulzSec.[17]

---

[11] Chris Davies, "Anonymous Denies Sony PSN 'We Are Legion' Calling Card," *SlashGear.com*, May 5, 2011. http://www.slashgear.com/anonymous-denies-sony-psn-we-are-legion-calling-card-05150280/.

[12] Sarah Purewal, "Sony Sues PS3 Hackers," *PCWorld.com*, January 12, 2011. http://www.pcworld.com/article/216547/Sony_Sues_PS3_Hackers.html.

[13] Michael Stone, "Anonymous #OpSony: DDoS Attacks Against Play Station Succeed," *Examin-er.com*, April 6, 2011. http://www.examiner.com/article/anonymous-opsony-ddos-attacks-against-playstation-succeed.

[14] Julianne Pepitone, "Group Claims Fresh Hack of 1 Million Sony Accounts," *CNN Money*, June 2, 2011. http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/index.htm.

[15] Kim Zetter, "FBI Arrests U.S. Suspect in LulzSec Sony Hack; Anonymous also Targeted," *Wired.com*, September 22, 2011. http://www.wired.com/threatlevel/2011/09/sony-hack-arrest/.

[16] Salvador Rodriquez, "LulzSec Hacker Sentenced to a Year in Federal Prison," *Los Angles Times*, April 18, 2013. http://articles.latimes.com/2013/apr/18/business/la-fi-tn-lulzsec-hacker-year-sentence-20130418.

[17] N. R. Kleinfield and Somini Sengupta, "Hacker, Informant and Party Boy of the Projects," *The New York Times*, March 8, 2012. http://www.nytimes.com/2012/03/09/technology/hacker-informant-and-party-boy-of-the-projects.html.

The Fallout

Following the data breaches, Sony offered its users compensation in the form of one year of free identity theft services, a month of free online gaming service, and couple games from a limited selection of games.[18] To date, no known credit fraud has occurred as a direct result of the Sony data breaches.

Sony was fined £250,000 (about $395,000) by the Information Commissioner's Office in the UK. Deputy Commissioner David Smith said that "the security measures were simply not good enough."[19] Other losses related to the attack are harder to quantify. While Sony estimates its direct losses at $171 million, it may be more difficult to quantify the impact of the series of data breaches on Sony's reputation.

TEST YOUR UNDERSTANDING

2. **a.** Who were the victims in the Sony breach?
b. How did the attackers steal the information from Sony? Explain.
c. What likely motivated the attackers?
d. What is SQL injection?
e. Were Sony's security measures strong enough? Why or why not?

1.2 EMPLOYEE AND EX-EMPLOYEE THREATS

Having looked at threats in general, at key security terminology, and at a particular compromise, we will now look at specific elements of the corporate threat environment. We will begin by looking inside the firm, at the threats created by employees. When firms began getting their own computers in the 1960s, they soon found that disgruntled and greedy employees and ex-employees are serious security threats. As firms have become more dependent on information technology, the threats from insiders have become more perilous.

Why Employees Are Dangerous

Employees and ex-employees are very dangerous for four reasons:

- They usually have extensive *knowledge* of systems.
- They often have the credentials needed to *access* sensitive parts of systems.
- They know corporate control mechanisms and so often know how to *avoid* detection.
- Finally, companies tend to *trust* their employees. In fact, when security insists that an employee behave in a particular way or explain an apparent security violation, it is common for the employee's manager to protect the employee against "security interference."

Employees and ex-employees are very dangerous because they have extensive knowledge of systems, have the credentials needed to access sensitive parts of systems, often know how to avoid detection, and can benefit from the trust that usually is accorded to "our people."

[18] Sony Online Entertainment LLC, "Customer Service Notification," *SOE.com*, May 2, 2011. https://www.soe.com/securityupdate/.
[19] BBC, "Sony Fined over 'Preventable' PlayStation Data Hack," *BBC.co.uk*, January 24, 2013. http://www.bbc.co.uk/news/technology-21160818.