



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 Chinnsamy, 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.

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 © 2015, 2013, 2010, 2004 by Pearson Education, Inc., One Lake Street, Upper Saddle River, New Jersey 07458. 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 likewise. To obtain permission(s) to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, One Lake Street, Upper Saddle River, New Jersey 07458, or you may fax your request to 201-236-3290.

Many of the designations by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed in initial caps or all caps.

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 xix

About the Authors xxv

Chapter 1 The Threat Environment 1

1.1 Introduction 2

Basic Security Terminology 2

THE THREAT ENVIRONMENT 2

SECURITY GOALS 3

COMPROMISES 3

COUNTERMEASURES 3

1.2 Employee And Ex-Employee Threats 9

Why Employees Are Dangerous 9

Employee Sabotage 11

Employee Hacking 12

Employee Financial Theft and Theft of Intellectual Property 12

Employee Extortion 13

Employee Sexual or Racial Harassment 14

Employee Computer and Internet Abuse 14

INTERNET ABUSE 14

NON-INTERNET COMPUTER ABUSE 15

Data Loss 15

Other "Internal" Attackers 16

1.3 Malware 16

Malware Writers 16

Viruses 16

Worms 18

Blended Threats 20

Payloads 20

Trojan Horses and Rootkits 20

NONMOBILE MALWARE 20

TROJAN HORSES 21

REMOTE ACCESS TROJANS 21

DOWNLOADERS 22

SPYWARE 22

ROOTKITS 23

Mobile Code 23

Social Engineering in Malware 23

SPAM 24

PHISHING 24

SPEAR PHISHING 26

HOAXES 27

1.4 Hackers And Attacks 27

Traditional Motives 27

Anatomy of a Hack 28

TARGET SELECTION 28

RECONNAISSANCE PROBES 29

THE EXPLOIT 30

SPOOFING 30

Social Engineering in an Attack 31

Denial-of-Service Attacks 33

Skill Levels 35

1.5 The Criminal Era 36

Dominance by Career Criminals 36

CYBERCRIME 36

INTERNATIONAL GANGS 37

BLACK MARKETS AND MARKET

SPECIALIZATION 38

Fraud, Theft, and Extortion 41

FRAUD 41

FINANCIAL AND INTELLECTUAL PROPERTY THEFT 41

EXTORTION AGAINST CORPORATIONS 42

Stealing Sensitive Data about Customers and Employees 43

CARDING 43

BANK ACCOUNT THEFT 43

ONLINE STOCK ACCOUNT THEFT 43

IDENTITY THEFT 43

THE CORPORATE CONNECTION 44

CORPORATE IDENTITY THEFT 44

1.6 Competitor Threats 45

Commercial Espionage 45

Denial-of-Service Attacks 46

1.7 Cyberwar And Cyberterror 47

Cyberwar 47

Cyberterror 48

1.8 Conclusion 49

Thought Questions 50 • *Hands-*

on Projects 51 • *Project*

Thought Questions 52 • *Case*

Study 52 • *Case Discussion*

Questions 53 • *Perspective*

Questions 53

Chapter 2 Planning and Policy 54

2.1 Introduction 55

Defense 55

Management Processes 56

MANAGEMENT IS THE HARD PART 56

COMPREHENSIVE SECURITY 56

WEAKEST-LINKS FAILURES 56

THE NEED TO PROTECT MANY

RESOURCES 57

The Need for a Disciplined Security
Management Process 58

The Plan–Protect–Respond
Cycle 59

PLANNING 59

PROTECTION 59

RESPONSE 60

Vision in Planning 61

VIEWING SECURITY AS AN ENabler 61

DEVELOPING POSITIVE VISIONS OF

USERS 63

Strategic IT Security Planning 63

2.2 Compliance Laws and
Regulations 64

Driving Forces 64

Sarbanes–Oxley 65

Privacy Protection Laws 67

Data Breach Notification
Laws 70

The Federal Trade Commission 70

Industry Accreditation 71

PCI-DSS 71

FISMA 71

2.3 Organization 72

Chief Security Officers 72

Should You Place Security
within IT? 72

LOCATING SECURITY WITHIN IT 72

PLACING SECURITY OUTSIDE IT 74

A HYBRID SOLUTION 74

Top Management Support 74

Relationships with Other
Departments 75

SPECIAL RELATIONSHIPS 75

ALL CORPORATE DEPARTMENTS 75

BUSINESS PARTNERS 76

Outsourcing IT Security 76

E-MAIL OUTSOURCING 76

MANAGED SECURITY SERVICE

PROVIDER 79

2.4 Risk Analysis 81

Reasonable Risk 81

Classic Risk Analysis

Calculations 82

ASSET VALUE 82

EXPOSURE FACTOR 82

SINGLE LOSS EXPECTANCY 82

ANNUALIZED PROBABILITY (OR RATE) OF
OCCURRENCE 82

ANNUALIZED LOSS EXPECTANCY 83

COUNTERMEASURE IMPACT 83

ANNUALIZED COUNTERMEASURE COST AND
NET VALUE 83

Problems with Classic Risk Analysis

Calculations 85

UNEVEN MULTIYEAR CASH FLOWS 85

TOTAL COST OF INCIDENT 85

MANY-TO-MANY RELATIONSHIPS
BETWEEN COUNTERMEASURES AND
RESOURCES 86

THE IMPOSSIBILITY OF COMPUTING
ANNUALIZED RATES OF
OCCURRENCE 87

THE PROBLEM WITH “HARD-HEADED
THINKING” 87

PERSPECTIVE 88

Responding to Risk 88

RISK REDUCTION 88

RISK ACCEPTANCE 88

RISK TRANSFERENCE (INSURANCE)	88
RISK AVOIDANCE	88
2.5 Technical Security Architecture	89
Technical Security Architectures	89
ARCHITECTURAL DECISIONS	90
DEALING WITH LEGACY SECURITY TECHNOLOGY	90
Principles	90
DEFENSE IN DEPTH	90
DEFENSE IN DEPTH VERSUS WEAKEST LINKS	90
SINGLE POINTS OF VULNERABILITY	91
MINIMIZING SECURITY BURDENS	92
REALISTIC GOALS	92
Elements of a Technical Security Architecture	92
BORDER MANAGEMENT	93
INTERNAL SITE SECURITY MANAGEMENT	93
MANAGEMENT OF REMOTE CONNECTIONS	93
INTERORGANIZATIONAL SYSTEMS	93
CENTRALIZED SECURITY MANAGEMENT	93
2.6 Policy-Driven Implementation	93
Policies	94
WHAT ARE POLICIES?	94
WHAT, NOT HOW	94
CLARITY	94
Categories of Security Policies	95
CORPORATE SECURITY POLICY	95
MAJOR POLICIES	95
ACCEPTABLE USE POLICY	96
POLICIES FOR SPECIFIC COUNTERMEASURES OR RESOURCES	96
Policy-Writing Teams	98
Implementation Guidance	98
NO GUIDANCE	98
STANDARDS AND GUIDELINES	98
Types of Implementation Guidance	100
PROCEDURES	100
PROCESSES	100
BASELINES	101
BEST PRACTICES AND RECOMMENDED PRACTICES	101
ACCOUNTABILITY	101
ETHICS	102
Exception Handling	103
Oversight	104
POLICIES AND OVERSIGHT	104
PROMULGATION	105
ELECTRONIC MONITORING	105
SECURITY METRICS	105
AUDITING	106
ANONYMOUS PROTECTED HOTLINE	106
BEHAVIORAL AWARENESS	108
FRAUD	108
SANCTIONS	109
2.7 Governance Frameworks	110
COSO	111
THE COSO FRAMEWORK	111
OBJECTIVES	112
REASONABLE ASSURANCE	112
COSO FRAMEWORK COMPONENTS	112
CobIT	113
THE COBIT FRAMEWORK	114
DOMINANCE IN THE UNITED STATES	114
The ISO/IEC 27000 Family	115
ISO/IEC 27002	115
ISO/IEC 27001	116
OTHER 27000 STANDARDS	116
2.8 Conclusion	117
<i>Thought Questions</i>	<i>117 •</i>
<i>Hands-on Projects</i>	<i>117 •</i>
<i>Project Thought Questions</i>	<i>118</i>
• <i>Case Study</i>	<i>119 • Case Discussion Questions</i>
• <i>Perspective Questions</i>	<i>120</i>
Chapter 3 Cryptography	121
3.1 What is Cryptography?	122
Encryption for Confidentiality	123
Terminology	123
PLAINTEXT	123
ENCRYPTION AND CIPHERTEXT	123
CIPHER	124
KEY	124
KEEPING THE KEY SECRET	124
The Simple Cipher	124
Cryptanalysis	125

Substitution and Transposition Ciphers	126
Substitution Ciphers	126
Transposition Ciphers	126
Real-world Encryption Ciphers and Codes	127
Symmetric Key Encryption	129
KEY LENGTH	129
Human Issues in Cryptography	131
3.2 Symmetric Key Encryption Ciphers	133
RC4	133
The Data Encryption Standard (DES)	134
56-BIT KEY SIZE	134
BLOCK ENCRYPTION	134
Triple DES (3DES)	135
168-BIT 3DES OPERATION	135
112-BIT 3DES	135
PERSPECTIVE ON 3DES	136
Advanced Encryption Standard (AES)	136
Other Symmetric Key Encryption Ciphers	136
3.3 Cryptographic System Standards	139
Cryptographic Systems	139
Initial Handshaking Stages	139
NEGOTIATION	139
INITIAL AUTHENTICATION	140
KEYING	140
Ongoing Communication	140
3.4 The Negotiation Stage	141
Cipher Suite Options	141
Cipher Suite Policies	142
3.5 Initial Authentication Stage	142
Authentication Terminology	142
Hashing	143
Initial Authentication with MS-CHAP	144
ON THE SUPPLICANT'S MACHINE: HASHING	144
ON THE VERIFIER SERVER	145
3.6 The Keying Stage	146
Session Keys	146
Public Key Encryption for Confidentiality	146
TWO KEYS	146
PROCESS	146
PADLOCK AND KEY ANALOGY	146
HIGH COST AND SHORT MESSAGE LENGTHS	147
RSA AND ECC	147
KEY LENGTH	148
Symmetric Key Keying Using Public Key Encryption	148
Symmetric Key Keying Using Diffie-Hellman Key Agreement	149
3.7 Message-By-Message Authentication	150
Electronic Signatures	150
Public Key Encryption for Authentication	150
Message-by-Message Authentication with Digital Signatures	151
DIGITAL SIGNATURES	151
HASHING TO PRODUCE THE MESSAGE DIGEST	151
SIGNING THE MESSAGE DIGEST TO PRODUCE THE DIGITAL SIGNATURE	151
SENDING THE MESSAGE WITH CONFIDENTIALITY	152
VERIFYING THE SUPPLICANT MESSAGE INTEGRITY	153
PUBLIC KEY ENCRYPTION FOR CONFIDENTIALITY AND AUTHENTICATION	153
Digital Certificates	154
CERTIFICATE AUTHORITIES	154
DIGITAL CERTIFICATE	155
VERIFYING THE DIGITAL CERTIFICATE	155
THE ROLES OF THE DIGITAL CERTIFICATE AND DIGITAL SIGNATURE	157
Key-Hashed Message Authentication Codes	158
THE PROBLEM WITH DIGITAL SIGNATURES	158
Creating and Testing the HMAC	158
Nonrepudiation	160

3.8 Quantum Security	162
3.9 Cryptographic Systems	163
Virtual Private Networks (VPNs)	164
Why VPNs?	164
Host-to-Host VPNs	164
Remote Access VPNs	165
Site-to-Site VPNs	165
3.10 SSL/TLS	166
Nontransparent Protection	166
Inexpensive Operation	167
SSL/TLS Gateways and Remote Access VPNs	167
VPN GATEWAY STANDARDS	168
AUTHENTICATION	168
CONNECTING THE CLIENT PC TO AUTHORIZED RESOURCES	168
SECURITY FOR SERVICES	168
BROWSER ON THE CLIENT	168
ADVANCED SERVICES REQUIRE ADMINISTRATOR PRIVILEGES ON PCs	170
PERSPECTIVE	171
3.11 IPsec	171
Attractions of IPsec	171
SSL/TLS GIVES NONTRANSPARENT TRANSPORT LAYER SECURITY	172
IPSEC: TRANSPARENT INTERNET LAYER SECURITY	172
IPSEC IN BOTH IPV4 AND IPV6	172
IPsec Transport Mode	173
HOST-TO-HOST SECURITY	173
END-TO-END PROTECTION	173
COST OF SETUP	173
IPSEC IN TRANSPORT MODE AND FIREWALLS	173
IPsec Tunnel Mode	174
PROTECTION IS PROVIDED BY IPSEC GATEWAYS	174
LESS EXPENSIVE THAN TRANSPORT MODE	174
FIREWALL-FRIENDLY PROTECTION	175
NO PROTECTION WITHIN THE TWO SITES	175
IPsec Security Associations (SAs)	175
SEPARATE SAs IN THE TWO DIRECTIONS	175
POLICY-BASED SA	176
3.12 Conclusion	176
Thought Questions	178
Hands-on Projects	179
Project Thought Questions	180
• Case Study	181
• Case Discussion Questions	182
• Perspective Questions	182
Chapter 4 Secure Networks	183
4.1 Introduction	184
Creating Secure Networks	184
AVAILABILITY	184
CONFIDENTIALITY	184
FUNCTIONALITY	185
ACCESS CONTROL	185
Future of Secure Networks	185
DEATH OF THE PERIMETER	185
RISE OF THE CITY	186
4.2 DoS Attacks	187
Denial of Service ... But Not an Attack	187
FAULTY CODING	187
REFERRALS FROM LARGE SITES	188
Goal of DoS Attacks	188
STOP CRITICAL SERVICES	188
DEGRADE SERVICES	188
Methods of DoS Attacks	188
DIRECT AND INDIRECT ATTACKS	190
INTERMEDIARY	192
REFLECTED ATTACK	194
SENDING MALFORMED PACKETS	195
Defending Against Denial-of-Service Attacks	196
BLACK HOLING	197
VALIDATING THE HANDSHAKE	198
RATE LIMITING	198
4.3 ARP Poisoning	199
Normal ARP Operation	199
THE PROBLEM	201
ARP Poisoning	201
ARP DoS Attack	203
Preventing ARP Poisoning	203
STATIC TABLES	203
LIMIT LOCAL ACCESS	204

4.4 Access Control for Networks 206

LAN Connections 206

Access Control Threats 206

Eavesdropping Threats 207

4.5 Ethernet Security 207

Ethernet and 802.1X 207

COST SAVINGS 208

CONSISTENCY 208

IMMEDIATE CHANGES 208

The Extensible Authentication Protocol (EAP) 209

EAP OPERATION 209

EXTENSIBILITY 210

RADIUS Servers 210

RADIUS AND EAP 211

4.6 Wireless Security 211

Wireless Attacks 212

Unauthorized Network Access 212

PREVENTING UNAUTHORIZED ACCESS 213

Evil Twin Access Points 215

Wireless Denial of Service 216

FLOOD THE FREQUENCY 216

FLOOD THE ACCESS POINT 218

SEND ATTACK COMMANDS 218

Wireless LAN Security with 802.11i 218

EAP'S NEED FOR SECURITY 219

ADDING SECURITY TO EAP 219

EAP-TLS AND PEAP 220

Core Wireless Security Protocols 221**Wired Equivalent Privacy (WEP) 221****Cracking WEP 221**

SHARED KEYS AND OPERATIONAL SECURITY 221

EXPLOITING WEP'S WEAKNESS 222

Perspective 223**Wi-Fi Protected Access (WPA™) 223****Pre-Shared Key (PSK) Mode 226****Wireless Intrusion Detection****Systems 228****False 802.11 Security Measures 229**

SPREAD SPECTRUM OPERATION AND SECURITY 229

TURNING OFF SSID BROADCASTING 229

MAC ACCESS CONTROL LISTS 229

Implementing 802.11i or WPA Is Easier 229**4.7 Conclusion 230***Thought Questions 232 •**Hands-on Projects 232 •**Project Thought Questions 233*• *Case Study 233 • Case Discus-**sion Questions 235 • Perspective**Questions 235***Chapter 5 Access Control 236****5.1 Introduction 237**

Access Control 237

Authentication, Authorizations, and Auditing 237

Authentication 238

Beyond Passwords 238

Two-Factor Authentication 238

Individual and Role-Based Access Control 238

Organizational and Human Controls 240

Military and National Security

Organization Access Controls 240

Multilevel Security 241

5.2 Physical Access and Security 242

Risk Analysis 242

ISO/IEC 9.1: Secure Areas 242

PHYSICAL SECURITY PERIMETER 242

PHYSICAL ENTRY CONTROLS 242

PUBLIC ACCESS, DELIVERY, AND LOADING AREAS 243

SECURING OFFICES, ROOMS, AND FACILITIES 243

PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS 244

RULES FOR WORKING IN SECURE AREAS 247

ISO/IEC 9.2 Equipment Security 247

EQUIPMENT SITING AND PROTECTION 247

SUPPORTING UTILITIES 248

CABLING SECURITY 248

SECURITY DURING OFF-SITE EQUIPMENT MAINTENANCE	248	SUBSEQUENT ACCESS ATTEMPTS	264
SECURITY OF EQUIPMENT OFF-PREMISES	248	ACCEPTANCE OR REJECTION	265
SECURE DISPOSAL OR REUSE OF EQUIPMENT	248	Biometric Errors	266
REMOVAL OF PROPERTY	248	FALSE ACCEPTANCE RATE	266
Other Physical Security Issues	249	FALSE REJECTION RATE	267
TERRORISM	249	WHICH IS WORSE?	267
PIGGYBACKING	249	VENDOR CLAIMS	267
MONITORING EQUIPMENT	249	FAILURE TO ENROLL	267
DUMPSTER™ DIVING	250	Verification, Identification, and Watch Lists	268
DESKTOP PC SECURITY	250	VERIFICATION	268
NOTEBOOK SECURITY	250	IDENTIFICATION	268
		WATCH LISTS	269
5.3 Passwords	251	Biometric Deception	270
Password-Cracking Programs	251	Biometric Methods	270
Password Policies	251	FINGERPRINT RECOGNITION	270
Password Use and Misuse	251	IRIS RECOGNITION	271
NOT USING THE SAME PASSWORD AT MULTIPLE SITES	252	FACE RECOGNITION	272
PASSWORD DURATION POLICIES	253	HAND GEOMETRY	273
POLICIES PROHIBITING SHARED ACCOUNTS	253	VOICE RECOGNITION	277
DISABLING PASSWORDS THAT ARE NO LONGER VALID	253	OTHER FORMS OF BIOMETRIC AUTHENTICATION	277
LOST PASSWORDS	254	5.6 Cryptographic Authentication	277
PASSWORD STRENGTH	256	Key Points from Chapter 3	277
PASSWORD AUDITING	256	Public Key Infrastructures	278
The End of Passwords?	257	THE FIRM AS A CERTIFICATE AUTHORITY	278
5.4 Access Cards and Tokens	258	CREATING PUBLIC KEY-PRIVATE KEY PAIRS	278
Access Cards	258	DISTRIBUTING DIGITAL CERTIFICATES	279
MAGNETIC STRIPE CARDS	259	ACCEPTING DIGITAL CERTIFICATES	279
SMART CARDS	259	CERTIFICATE REVOCATION STATUS	279
CARD READER COSTS	259	PROVISIONING	279
Tokens	259	THE PRIME AUTHENTICATION PROBLEM	279
ONE-TIME-PASSWORD TOKENS	260	5.7 Authorization	280
USB TOKENS	260	The Principle of Least Permissions	280
Proximity Access Tokens	260	5.8 Auditing	282
Addressing Loss and Theft	260	Logging	282
PHYSICAL DEVICE CANCELLATION	260	Log Reading	282
TWO-FACTOR AUTHENTICATION	260	REGULAR LOG READING	282
5.5 Biometric Authentication	263		
Biometrics	263		
Biometric Systems	264		
INITIAL ENROLLMENT	264		

PERIODIC EXTERNAL AUDITS OF LOG FILE ENTRIES 283
AUTOMATIC ALERTS 283

5.9 Central Authentication Servers 283

The Need for Centralized Authentication 283
Kerberos 284

5.10 Directory Servers 285

What Are Directory Servers? 286
Hierarchical Data Organization 286
Lightweight Data Access Protocol 287
Use by Authentication Servers 287
Active Directory 287
ACTIVE DIRECTORY DOMAINS 287

Trust 289

5.11 Full Identity Management 290

Other Directory Servers and Metadirectories 290
Federated Identity Management 291

THE SECURITY ASSERTION MARKUP LANGUAGE 292
PERSPECTIVE 292

Identity Management 293

BENEFITS OF IDENTITY MANAGEMENT 293
WHAT IS IDENTITY? 293
IDENTITY MANAGEMENT 294

Trust and Risk 295

5.12 Conclusion 296

Thought Questions 298 •
Hands-on Projects 298 •
Project Thought Questions 300
• *Case Study 300* • *Case Discussion Questions 301* • *Perspective Questions 302*

Chapter 6 Firewalls 303

6.1 Introduction 304

Basic Firewall Operation 304
The Danger of Traffic Overload 308
Firewall Filtering Mechanisms 310

6.2 Static Packet Filtering 310

Looking at Packets One at a Time 311

Looking Only at Some Fields in the Internet and Transport Headers 311

Usefulness of Static Packet Filtering 311

Perspective 313

6.3 Stateful Packet Inspection 313

Basic Operation 313

CONNECTIONS 313
STATES 313
STATEFUL PACKET INSPECTION WITH TWO STATES 314
REPRESENTING CONNECTIONS 315

Packets That Do Not Attempt to Open Connections 315

TCP CONNECTIONS 318
UDP AND ICMP CONNECTIONS 318
ATTACK ATTEMPTS 319
PERSPECTIVE 319

Packets That Do Attempt to Open a Connection 319

Access Control Lists (ACLs) for Connection-Opening Attempts 320

WELL-KNOWN PORT NUMBERS 321
ACCESS CONTROL LISTS FOR INGRESS FILTERING 322
IF-THEN FORMAT 322
PORTS AND SERVER ACCESS 322
DISALLOW ALL CONNECTIONS 323

Perspective on SPI Firewalls 324

LOW COST 324
SAFETY 324
DOMINANCE 324

6.4 Network Address

Translation 324

Sniffers 325

NAT OPERATION 325
PACKET CREATION 325
NETWORK AND PORT ADDRESS TRANSLATION (NAT/PAT) 325
TRANSLATION TABLE 325
RESPONSE PACKET 325
RESTORATION 325
PROTECTION 326

- Perspective on NAT 326
 - NAT/PAT 326
 - TRANSPARENCY 326
 - NAT TRAVERSAL 326
- 6.5 Application Proxy Firewalls and Content Filtering 326
 - Application Proxy Firewall Operation 326
 - OPERATIONAL DETAILS 326
 - APPLICATION PROXY PROGRAMS VERSUS APPLICATION PROXY FIREWALLS 327
 - PROCESSING-INTENSIVE OPERATION 327
 - ONLY A FEW APPLICATIONS CAN BE PROXIED 327
 - TWO COMMON USES 327
 - Application Content Filtering in Stateful Packet Inspection Firewalls 328
 - Application Content Filtering for HTTP 329
 - Client Protections 330
 - Server Protections 331
 - Other Protections 333
- 6.6 Intrusion Detection Systems and Intrusion Prevention Systems 334
 - Intrusion Detection Systems 334
 - FIREWALLS VERSUS IDSs 334
 - FALSE POSITIVES (FALSE ALARMS) 334
 - HEAVY PROCESSING REQUIREMENTS 336
 - Intrusion Prevention Systems 336
 - ASICs FOR FASTER PROCESSING 337
 - THE ATTACK IDENTIFICATION CONFIDENCE SPECTRUM 337
 - IPS Actions 337
 - DROPPING PACKETS 337
 - LIMITING TRAFFIC 337
- 6.7 Antivirus Filtering and Unified Threat Management 337
- 6.8 Firewall Architectures 342
 - Types of Firewalls 342
 - MAIN BORDER FIREWALLS 342
 - SCREENING BORDER ROUTERS 342
 - INTERNAL FIREWALLS 342
 - HOST FIREWALLS 342
 - DEFENSE IN DEPTH 343
 - The Demilitarized Zone (DMZ) 343
 - SECURITY IMPLICATIONS 344
 - HOSTS IN THE DMZ 344
- 6.9 Firewall Management 345
 - Defining Firewall Policies 345
 - WHY USE POLICIES? 345
 - EXAMPLES OF POLICIES 345
 - Implementation 347
 - FIREWALL HARDENING 347
 - CENTRAL FIREWALL MANAGEMENT SYSTEMS 347
 - FIREWALL POLICY DATABASE 348
 - VULNERABILITY TESTING AFTER CONFIGURATION 349
 - CHANGE AUTHORIZATION AND MANAGEMENT 349
 - READING FIREWALL LOGS 349
 - Reading Firewall Logs 350
 - Log Files 350
 - Sorting the Log File by Rule 350
 - Echo Probes 351
 - External Access to All Internal FTP Servers 352
 - Attempted Access to Internal Webservers 352
 - Incoming Packet with a Private IP Source Address 352
 - Lack of Capacity 352
 - Perspective 352
 - Sizes of Log Files 353
 - Logging All Packets 353
- 6.10 Firewall Filtering Problems 353
 - The Death of the Perimeter 354
 - AVOIDING THE BORDER FIREWALL 354
 - EXTENDING THE PERIMETER 355
 - PERSPECTIVE 355
 - Attack Signatures versus Anomaly Detection 355
 - ZERO-DAY ATTACKS 356
 - ANOMALY DETECTION 356
 - ACCURACY 356

6.11 Conclusion 356

- Thought Questions 358* •
- Hands-on Projects 359* •
- Project Thought Questions 361*
 - *Case Study 361* • *Case Discussion Questions 363* • *Perspective Questions 363*

Chapter 7 Host Hardening 364

7.1 Introduction 365

- What Is a Host? 365**
- The Elements of Host Hardening 365**
- Security Baselines and Images 366**
- Virtualization 367**
 - VIRTUALIZATION ANALOGY 368
 - BENEFITS OF VIRTUALIZATION 369
- Systems Administrators 369**

7.2 Important Server Operating Systems 375

- Windows Server Operating Systems 375**
 - THE WINDOWS SERVER USER INTERFACE 375
 - START → ADMINISTRATIVE TOOLS 376
 - MICROSOFT MANAGEMENT CONSOLES (MMCs) 376
- UNIX (Including Linux) Servers 377**
 - MANY VERSIONS 378
 - LINUX 379
 - UNIX USER INTERFACES 380

7.3 Vulnerabilities and Patches 381

- Vulnerabilities and Exploits 381**
- Fixes 381**
 - WORK-AROUNDS 385
 - PATCHES 385
 - SERVICE PACKS 386
 - VERSION UPGRADES 386
- The Mechanics of Patch Installation 386**
 - MICROSOFT WINDOWS SERVER 386
 - LINUX RPM PROGRAM 386
- Problems with Patching 386**
 - THE NUMBER OF PATCHES 386
 - COST OF PATCH INSTALLATION 387

- PRIORITIZING PATCHES 387
- PATCH MANAGEMENT SERVERS 387
- THE RISKS OF PATCH INSTALLATION 388

7.4 Managing Users and Groups 388

- The Importance of Groups in Security Management 388**
- Creating and Managing Users and Groups in Windows 389**
 - THE ADMINISTRATOR ACCOUNT 389
 - MANAGING ACCOUNTS 389
 - CREATING USERS 390
 - WINDOWS GROUPS 390

7.5 Managing Permissions 391

- Permissions 391**
- Assigning Permissions in Windows 392**
 - DIRECTORY PERMISSIONS 392
 - WINDOWS PERMISSIONS 393
 - ADDING USERS AND GROUPS 393
 - INHERITANCE 393
 - DIRECTORY ORGANIZATION 393

Assigning Groups and Permissions in UNIX 394

- NUMBER OF PERMISSIONS 395
- NUMBER OF ACCOUNTS OR GROUPS 395

7.6 Creating Strong Passwords 395

- Creating and Storing Passwords 396**
 - CREATING A PASSWORD HASH 396
 - STORING PASSWORDS 396
 - STEALING PASSWORDS 397

Password-Cracking Techniques 397

- BRUTE-FORCE GUESSING 397
- DICTIONARY ATTACKS ON COMMON WORD PASSWORDS 399
- HYBRID DICTIONARY ATTACKS 400
- RAINBOW TABLES 401
- TRULY RANDOM PASSWORDS 401
- TESTING AND ENFORCING THE STRENGTH OF PASSWORDS 402
- OTHER PASSWORD THREATS 402

7.7 Testing For Vulnerabilities 403

- Windows Client PC Security 404**
- Client PC Security Baselines 404**
- The Windows Action Center 404**

Windows Firewall	405	MINIMIZE APPLICATIONS	425
Automatic Updates	406	SECURITY BASELINES FOR APPLICATION MINIMIZATION	426
Antivirus and Spyware Protection	407	CREATE A SECURE CONFIGURATION	426
Implementing Security Policy	408	INSTALL APPLICATION PATCHES AND UPDATES	427
PASSWORD POLICIES	408	MINIMIZE THE PERMISSIONS OF APPLICATIONS	427
ACCOUNT POLICIES	408	ADD APPLICATION-LEVEL AUTHENTICATION, AUTHORIZATIONS, AND AUDITING	427
AUDIT POLICIES	408	IMPLEMENT CRYPTOGRAPHIC SYSTEMS	427
Protecting Notebook Computers	410	Securing Custom Applications	427
THREATS	410	NEVER TRUST USER INPUT	428
BACKUP	410	BUFFER OVERFLOW ATTACKS	428
POLICIES FOR SENSITIVE DATA	411	LOGIN SCREEN BYPASS ATTACKS	429
TRAINING	411	CROSS-SITE SCRIPTING ATTACKS	429
COMPUTER RECOVERY SOFTWARE	411	SQL INJECTION ATTACKS	429
Centralized PC Security		AJAX MANIPULATION	430
Management	411	TRAINING IN SECURE COMPUTING	430
STANDARD CONFIGURATIONS	412	8.2 WWW and E-Commerce Security	433
NETWORK ACCESS CONTROL	412	The Importance of WWW and E-Commerce Security	433
WINDOWS GROUP POLICY OBJECTS	412	WWW Service versus E-Commerce Service	433
7.8 Conclusion	415	WWW SERVICE	433
<i>Thought Questions</i>	416 • <i>Hands-on Projects</i>	E-COMMERCE SERVICE	433
<i>Thought Questions</i>	417 • <i>Case Study</i>	EXTERNAL ACCESS	434
<i>Thought Questions</i>	419 • <i>Case Discussion Questions</i>	CUSTOM PROGRAMS	435
<i>Thought Questions</i>	419	Some Webserver Attacks	435
Chapter 8 Application Security	420	WEBSITE DEFAACEMENT	435
8.1 Application Security and Hardening	421	BUFFER OVERFLOW ATTACK TO LAUNCH A COMMAND SHELL	436
Executing Commands with the Privileges of a Compromised Application	421	DIRECTORY TRAVERSAL ATTACK	436
Buffer Overflow Attacks	421	THE DIRECTORY TRAVERSAL WITH HEXADECIMAL CHARACTER ESCAPES	436
BUFFERS AND OVERFLOWS	422	UNICODE DIRECTORY TRAVERSAL	437
STACKS	422	Patching the Webserver and E-Commerce Software and Its Components	437
RETURN ADDRESS	422	E-COMMERCE SOFTWARE VULNERABILITIES	437
THE BUFFER AND BUFFER OVERFLOW	422	Other Website Protections	438
EXECUTING ATTACK CODE	422	WEBSITE VULNERABILITY ASSESSMENT TOOLS	438
AN EXAMPLE: THE IIS IPP BUFFER OVERFLOW ATTACK	423		
Few Operating Systems, Many Applications	423		
Hardening Applications	424		
UNDERSTAND THE SERVER'S ROLE AND THREAT ENVIRONMENT	424		
THE BASICS	425		

WEBSITE ERROR LOGS	438
WEBSERVER-SPECIFIC APPLICATION PROXY FIREWALLS	439
Controlling Deployment	439
DEVELOPMENT SERVERS	439
TESTING SERVERS	439
PRODUCTION SERVERS	439
8.3 Web Browser Attacks	440
BROWSER THREATS	440
MOBILE CODE	440
MALICIOUS LINKS	442
OTHER CLIENT-SIDE ATTACKS	442
Enhancing Browser Security	444
PATCHING AND UPGRADING	444
CONFIGURATION	444
INTERNET OPTIONS	444
SECURITY TAB	444
PRIVACY TAB	448
8.4 E-Mail Security	449
E-Mail Content Filtering	449
MALICIOUS CODE IN ATTACHMENTS AND HTML BODIES	449
SPAM	449
INAPPROPRIATE CONTENT	450
EXTRUSION PREVENTION	450
PERSONALLY IDENTIFIABLE INFORMATION	450
Where to Do E-Mail Malware and Spam Filtering	451
E-Mail Encryption	452
TRANSMISSION ENCRYPTION	452
MESSAGE ENCRYPTION	452
8.5 Voice over IP Security	454
Sending Voice between Phones	454
Transport and Signaling	455
SIP and H.323	455
Registration	455
SIP Proxy Servers	455
PSTN Gateway	456
VoIP Threats	456
Eavesdropping	456
Denial-of-Service Attacks	457
Caller Impersonation	457
Hacking and Malware Attacks	457
Toll Fraud	458
Spam over IP Telephony	458
New Threats	458
Implementing VoIP Security	459
Authentication	459
Encryption for Confidentiality	460
Firewalls	460
NAT Problems	460
Separation: Anticonvergence	460
The Skype VoIP Service	461
8.6 Other User Applications	462
Instant Messaging	462
TCP/IP Supervisory Applications	464
8.7 Conclusion	465
<i>Thought Questions</i>	<i>466 • Hands- on Projects 466 • Project Thought Questions 468 • Case Study 468 • Case Discussion Questions 469 • Perspective Questions 469</i>
Chapter 9 Data Protection	470
9.1 Introduction	471
Data's Role in Business	471
SONY DATA BREACHES	471
Securing Data	472
9.2 Data Protection: Backup	472
The Importance of Backup	472
Threats	472
Scope of Backup	472
FILE/DIRECTORY DATA BACKUP	473
IMAGE BACKUP	473
SHADOWING	473
Full versus Incremental Backups	475
Backup Technologies	476
LOCAL BACKUP	476
CENTRALIZED BACKUP	478
CONTINUOUS DATA PROTECTION	478
INTERNET BACKUP SERVICE	479
MESH BACKUP	479
9.3 Backup Media and Raid	480
MAGNETIC TAPE	480
CLIENT PC BACKUP	481

Disk Arrays—RAID	481		
Raid Levels	482		
No RAID	482		
RAID 0	483		
RAID 1	483		
RAID 5	485		
9.4 Data Storage Policies	488		
BACKUP CREATION POLICIES	488		
RESTORATION POLICIES	488		
MEDIA STORAGE LOCATION POLICIES	488		
ENCRYPTION POLICIES	489		
ACCESS CONTROL POLICIES	489		
RETENTION POLICIES	490		
AUDITING BACKUP POLICY COMPLIANCE	490		
E-Mail Retention	490		
THE BENEFIT OF RETENTION	490		
THE DANGERS OF RETENTION	490		
ACCIDENTAL RETENTION	491		
THIRD-PARTY E-MAIL RETENTION	491		
LEGAL ARCHIVING REQUIREMENTS	491		
U.S. FEDERAL RULES OF CIVIL PROCEDURE	491		
MESSAGE AUTHENTICATION	493		
DEVELOPING POLICIES AND PROCESSES	493		
User Training	493		
Spreadsheets	494		
VAULT SERVER ACCESS CONTROL	494		
OTHER VAULT SERVER PROTECTIONS	495		
9.5 Database Security	495		
Relational Databases	496		
LIMITING THE VIEW OF DATA	496		
Database Access Control	500		
DATABASE ACCOUNTS	500		
SQL INJECTION ATTACKS	500		
Database Auditing	501		
WHAT TO AUDIT	501		
TRIGGERS	502		
Database Placement and Configuration	503		
CHANGE THE DEFAULT PORT	504		
Data Encryption	504		
KEY ESCROW	504		
FILE/DIRECTORY ENCRYPTION VERSUS WHOLE-DISK ENCRYPTION	506		
			PROTECTING ACCESS TO THE COMPUTER 506
			DIFFICULTIES IN FILE SHARING 506
		9.6 Data Loss Prevention	506
		Data Collection	506
		PERSONALLY IDENTIFIABLE INFORMATION	507
		DATA MASKING	507
		Information Triangulation	509
		BUY OR SELL DATA	510
		Document Restrictions	511
		DIGITAL RIGHTS MANAGEMENT	511
		DATA EXTRUSION MANAGEMENT	512
		EXTRUSION PREVENTION	512
		Data Loss Prevention Systems	512
		DLP AT THE GATEWAY	514
		DLP ON CLIENTS	514
		DLP FOR DATA STORAGE	514
		DLP MANAGER	514
		WATERMARKS	514
		REMOVABLE MEDIA CONTROLS	515
		PERSPECTIVE	516
		Employee Training	516
		SOCIAL NETWORKING	516
		Data Destruction	517
		NOMINAL DELETION	517
		BASIC FILE DELETION	518
		WIPING/CLEARING	519
		DESTRUCTION	519
		9.7 Conclusion	520
		<i>Thought Questions</i>	520 •
		<i>Hands-on Projects</i>	521 •
		<i>Project Thought Questions</i>	522
		• <i>Case Study</i>	522 • <i>Case Discus-</i>
		<i>sion Questions</i>	524 • <i>Perspective</i>
		<i>Questions</i>	524
		Chapter 10 Incident and Disaster Response	525
		10.1 Introduction	526
		Walmart and Hurricane Katrina	526
		Incidents Happen	527
		Incident Severity	527
		FALSE ALARMS	527
		MINOR INCIDENTS	527
		MAJOR INCIDENTS	527
		DISASTERS	529

Speed and Accuracy	530
SPEED IS OF THE ESSENCE	530
SO IS ACCURACY	530
PLANNING	531
REHEARSAL	531
10.2 The Intrusion Response Process	
For Major Incidents	532
Detection, Analysis, and	
Escalation	532
DETECTION	532
ANALYSIS	534
ESCALATION	534
Containment	534
DISCONNECTION	534
BLACK-HOLING THE ATTACKER	534
CONTINUING TO COLLECT DATA	534
Recovery	535
REPAIR DURING CONTINUING SERVER	
OPERATION	535
RESTORATION FROM	
BACKUP TAPES	535
TOTAL SOFTWARE REINSTALLATION	536
Apology	536
Punishment	536
PUNISHING EMPLOYEES	536
THE DECISION TO PURSUE	
PROSECUTION	537
COLLECTING AND MANAGING	
EVIDENCE	537
Postmortem Evaluation	539
Organization of the CSIRT	539
Legal Considerations	540
Criminal versus Civil Law	540
Jurisdictions	541
The U.S. Federal Judicial	
System	542
U.S. State and Local Laws	542
International Law	543
Evidence and Computer	
Forensics	545
U.S. Federal Cybercrime Laws	546
COMPUTER HACKING, MALWARE	
ATTACKS, DENIAL-OF-SERVICE ATTACKS,	
AND OTHER ATTACKS (18 U.S.C.	
§ 1030)	546
HACKING	547
DENIAL-OF-SERVICE AND MALWARE	
ATTACKS	547
DAMAGE THRESHOLDS	547
Confidentiality in Message	
Transmission	548
Other Federal Laws	548
10.3 Intrusion Detection Systems	548
Functions of an IDS	549
LOGGING (DATA COLLECTION)	549
AUTOMATED ANALYSIS BY THE IDS	550
ACTIONS	550
LOG SUMMARY REPORTS	550
SUPPORT FOR INTERACTIVE MANUAL LOG	
ANALYSIS	550
Distributed IDSs	551
AGENTS	551
MANAGER AND INTEGRATED LOG FILE	551
BATCH VERSUS REAL-TIME DATA	
TRANSFER	551
SECURE MANAGER-AGENT	
COMMUNICATION	552
VENDOR COMMUNICATION	552
Network IDSs	552
STAND-ALONE NIDSs	552
SWITCH AND ROUTER NIDSs	552
STRENGTHS OF NIDSs	552
WEAKNESSES OF NIDSs	552
HOST IDSs	553
ATTRACTION OF HIDSs	553
WEAKNESSES OF HOST IDSs	554
HOST IDSs: OPERATING SYSTEM	
MONITORS	554
Log Files	554
TIME-STAMPED EVENTS	554
INDIVIDUAL LOGS	554
INTEGRATED LOGS	554
MANUAL ANALYSIS	556
Managing IDSs	557
TUNING FOR PRECISION	557
Honeypots	558
10.4 Business Continuity	
Planning	563
Principles of Business Continuity	
Management	565
PEOPLE FIRST	565
REDUCED CAPACITY IN DECISION	
MAKING	565
AVOIDING RIGIDITY	565

COMMUNICATION, COMMUNICATION,
COMMUNICATION 565

Business Process Analysis 566

IDENTIFICATION OF BUSINESS PROCESSES
AND THEIR INTERRELATIONSHIPS 566

PRIORITIZATION OF BUSINESS
PROCESSES 566

SPECIFY RESOURCE NEEDS 566

SPECIFY ACTIONS AND SEQUENCES 566

Testing and Updating the Plan 566

10.5 IT Disaster Recovery 567

Types of Backup Facilities 568

HOT SITES 568

COLD SITES 568

SITE SHARING WITH CONTINUOUS DATA
PROTECTION 568

LOCATION OF THE SITES 569

Office PCs 572

DATA BACKUP 572

NEW COMPUTERS 572

WORK ENVIRONMENT 572

Restoration of Data and Programs 572

**Testing the IT Disaster Recovery
Plan 573**

10.6 Conclusion 573

Thought Questions 574 •

Hands-on Projects 574 •

Project Thought Questions 575

• Case Study 575 • Case Discus-

*sion Questions 577 • Perspective
Questions 577*

Module A Networking Concepts 578

A.1 Introduction 578

A.2 A Sampling of Networks 579

A Simple Home Network 579

THE ACCESS ROUTER 579

PERSONAL COMPUTERS 580

UTP WIRING 580

INTERNET ACCESS LINE 581

A Building LAN 581

A Firm's Wide Area Networks 582

The Internet 584

Applications 586

**A.3 Network Protocols and
Vulnerabilities 587**

Inherent Security 587

Security Explicitly Designed into the
Standard 587

Security in Older Versions of the
Standard 587

Defective Implementation 588

**A.4 Core Layers in Layered Standards
Architectures 588**

A.5 Standards Architectures 589

The TCP/IP Standards Architecture 589

The OSI Standards Architecture 590

The Hybrid TCP/IP-OSI
Architecture 590

A.6 Single-Network Standards 590

The Data Link Layer 591

The Physical Layer 591

UTP 591

OPTICAL FIBER 591

WIRELESS TRANSMISSION 592

SWITCH SUPERVISORY FRAMES 592

A.7 Internetworking Standards 593

A.8 The Internet Protocol 594

The IP Version 4 Packet 594

The First Row 594

The Second Row 595

The Third Row 595

Options 596

The Source and Destination IP
Addresses 596

Masks 596

IP Version 6 597

IPsec 598

**A.9 The Transmission Control
Protocol 599**

TCP: A Connection-Oriented and
Reliable Protocol 599

CONNECTIONLESS AND CONNECTION-
ORIENTED PROTOCOLS 599

RELIABILITY 601

Flag Fields 602

Sequence Number Field 602

Acknowledgment Number Field 603

Window Field	603	Simple Network Management Protocol	612
Options	604	A.12 Application Standards	613
Port Numbers	604	HTTP AND HTML	613
PORT NUMBERS ON SERVERS	604	E-MAIL	614
PORT NUMBERS ON CLIENTS	605	TELNET, FTP, AND SSH	615
SOCKETS	605	OTHER APPLICATION STANDARDS	615
TCP Security	606	A.13 Conclusion	615
A.10 The User Datagram Protocol	606	<i>Hands-on Projects</i>	615 •
A.11 TCP/IP Supervisory Standard	608	<i>Project Thought Questions</i>	617 •
Internet Control Message Protocol	608	<i>Perspective Questions</i>	617
The Domain Name System	609	Glossary	618
Dynamic Host Configuration Protocol	610	Index	635
Dynamic Routing Protocols	611		

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.

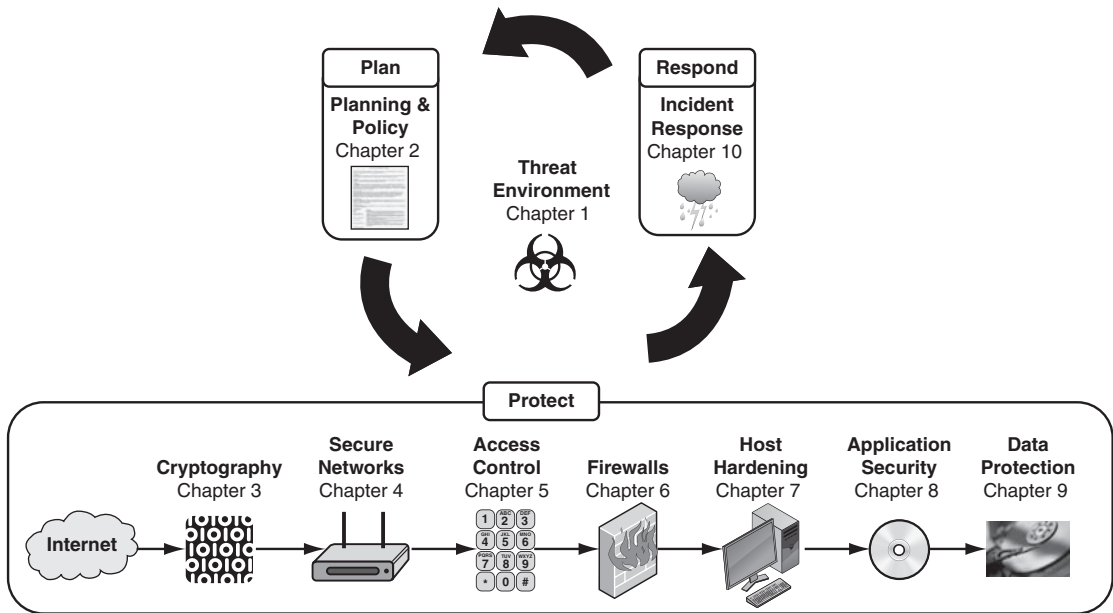
BALANCING TECHNICAL AND MANAGERIAL CONTENT Our students are going to need jobs. When you ask working IT security professionals what they are looking for in a new hire, they give similar responses. They want proactive workers who can take initiative, learn on their own, have strong technical skills, and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

- 1.1 Introduction
- 1.2 Employee and Ex-Employee Threats
- 1.3 Malware
- 1.4 Hackers and Attacks
- 1.5 The Criminal Era
- 1.6 Competitor Threats
- 1.7 Cyberwar and Cyberterror
- 1.8 Conclusion

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/#QuSrgtEootxXhtl.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.*

A screenshot of a normal login form. It has two input fields: 'Username:' with the value 'boyle02' and 'Password:' with the value '12345678'.

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

A screenshot of a login form demonstrating SQL injection. The 'Username:' field contains 'boyle02' and the 'Password:' field contains 'whatever' or 1=1--'.

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 jail-breaking 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,” *Examiner.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 Rodriguez, “LulzSec Hacker Sentenced to a Year in Federal Prison,” *Los Angeles Times*, April 18, 2013. <http://articles.latimes.com/2013/apr/18/business/la-fi-tn-lulzsec-hacker-year-sentence-20130418>.

¹⁷ N. R. Kleinfeld 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>.