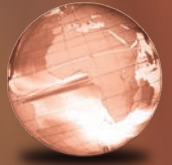


GLOBAL
EDITION



Corporate Computer Security

FOURTH EDITION



Randall J. Boyle | Raymond R. Panko

ALWAYS LEARNING

PEARSON

Fourth Edition

Corporate Computer Security

Global Edition

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

Head of Learning Asset Acquisition, Global Edition:
Laura Dent
Assistant Acquisitions Editor, Global Edition: Debapriya Mukherjee
Project Editor, Global Edition: Amrita Naskar
Media Producer, Global Edition: Vikram Kumar
Senior Manufacturing Controller, Production, Global Edition:
Trudy Kimber
Cover Designer: PreMediaGlobal
Cover Image: Devis Da Fre'/Shutterstock
Digital Production Project Manager: Lisa Rinaldi

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

Pearson Education Limited
Edinburgh Gate
Harlow
Essex CM20 2JE
England

and Associated Companies throughout the world

Visit us on the World Wide Web at: www.pearsonglobaleditions.com

© Pearson Education Limited 2015

The rights of Randall J. Boyle and Raymond R. Panko to be identified as the authors of this work have been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

Authorized adaptation from the United States edition, entitled Corporate Computer Security, 4/e, ISBN 978-0-13-354519-7, by Randall J. Boyle and Raymond R. Panko, published by Pearson Education © 2015.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without either the prior written permission of the publisher or a license permitting restricted copying in the United Kingdom issued by the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC 1N 8TS.

All trademarks used herein are the property of their respective owners. The use of any trademark in this text does not vest in the author or publisher any trademark ownership rights in such trademarks, nor does the use of such trademarks imply any affiliation with or endorsement of this book by such owners.

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® and Windows® 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.

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.

ISBN 10: 1-292-06045-X
ISBN 13: 978-1-292-06045-3 (Print)
ISBN 13: 978-1-292-06659-2 (PDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

10 9 8 7 6 5 4 3 2 1
14 13 12 11 10

Typeset in Times, 10/12 by Integra Software Services Pvt. Ltd
Printed and bound by Courier Westford in the United States of America

CONTENTS

Preface 19

About the Authors 25

Chapter 1 The Threat Environment 27

1.1 Introduction 28

Basic Security Terminology 28

THE THREAT ENVIRONMENT 28

SECURITY GOALS 29

COMPROMISES 29

COUNTERMEASURES 29

1.2 Employee And Ex-Employee Threats 35

Why Employees Are Dangerous 35

Employee Sabotage 37

Employee Hacking 38

Employee Financial Theft and Theft of Intellectual Property 38

Employee Extortion 39

Employee Sexual or Racial

Harassment 40

Employee Computer and Internet Abuse 40

INTERNET ABUSE 40

NON-INTERNET COMPUTER ABUSE 41

Data Loss 41

Other “Internal” Attackers 42

1.3 Malware 42

Malware Writers 42

Viruses 42

Worms 44

Blended Threats 46

Payloads 46

Trojan Horses and Rootkits 46

NONMOBILE MALWARE 46

TROJAN HORSES 47

REMOTE ACCESS TROJANS 47

DOWNLOADERS 48

SPYWARE 48

ROOTKITS 49

Mobile Code 49

Social Engineering in Malware 49

SPAM 50

PHISHING 50

SPEAR PHISHING 52

HOAXES 53

1.4 Hackers And Attacks 53

Traditional Motives 53

Anatomy of a Hack 54

TARGET SELECTION 54

RECONNAISSANCE PROBES 55

THE EXPLOIT 56

SPOOFING 56

Social Engineering in an Attack 57

Denial-of-Service Attacks 59

Skill Levels 61

1.5 The Criminal Era 62

Dominance by Career Criminals 62

CYBERCRIME 62

INTERNATIONAL GANGS 63

BLACK MARKETS AND MARKET SPECIALIZATION 64

Fraud, Theft, and Extortion 67

FRAUD 67

FINANCIAL AND INTELLECTUAL PROPERTY THEFT 67

EXTORTION AGAINST CORPORATIONS 68

Stealing Sensitive Data about Customers and Employees 69

CARDING 69

BANK ACCOUNT THEFT 69

ONLINE STOCK ACCOUNT THEFT 69

IDENTITY THEFT 69

THE CORPORATE CONNECTION 70

CORPORATE IDENTITY THEFT 70

1.6 Competitor Threats 71

Commercial Espionage 71

Denial-of-Service Attacks 72

1.7 Cyberwar And Cyberterror 73

Cyberwar 73

Cyberterror 74

1.8 Conclusion 75

Thought Questions 76 • *Hands-*

on Projects 77 • *Project*

Thought Questions 78 • *Case*

Study 78 • *Case Discussion*

Questions 79 • *Perspective*

Questions 79

Chapter 2 Planning and Policy 80

2.1 Introduction 81

Defense 81

Management Processes 82

MANAGEMENT IS THE HARD PART 82

COMPREHENSIVE SECURITY 82

WEAKEST-LINKS FAILURES 82

THE NEED TO PROTECT MANY

RESOURCES 83

The Need for a Disciplined Security
Management Process 84

The Plan–Protect–Respond
Cycle 85

PLANNING 85

PROTECTION 85

RESPONSE 86

Vision in Planning 87

VIEWING SECURITY AS AN ENABLER 87

DEVELOPING POSITIVE VISIONS OF
USERS 89

Strategic IT Security Planning 89

2.2 Compliance Laws and
Regulations 90

Driving Forces 90

Sarbanes–Oxley 91

Privacy Protection Laws 93

Data Breach Notification
Laws 96

The Federal Trade Commission 96

Industry Accreditation 97

PCI-DSS 97

FISMA 97

2.3 Organization 98

Chief Security Officers 98

Should You Place Security
within IT? 98

LOCATING SECURITY WITHIN IT 98

PLACING SECURITY OUTSIDE IT 100

A HYBRID SOLUTION 100

Top Management Support 100

Relationships with Other
Departments 101

SPECIAL RELATIONSHIPS 101

ALL CORPORATE DEPARTMENTS 101

BUSINESS PARTNERS 102

Outsourcing IT Security 102

E-MAIL OUTSOURCING 102

MANAGED SECURITY SERVICE

PROVIDER 105

2.4 Risk Analysis 107

Reasonable Risk 107

Classic Risk Analysis
Calculations 108

ASSET VALUE 108

EXPOSURE FACTOR 108

SINGLE LOSS EXPECTANCY 108

ANNUALIZED PROBABILITY (OR RATE) OF
OCCURRENCE 108

ANNUALIZED LOSS EXPECTANCY 109

COUNTERMEASURE IMPACT 109

ANNUALIZED COUNTERMEASURE COST AND
NET VALUE 109

Problems with Classic Risk Analysis
Calculations 111

UNEVEN MULTIYEAR CASH FLOWS 111

TOTAL COST OF INCIDENT 111

MANY-TO-MANY RELATIONSHIPS
BETWEEN COUNTERMEASURES AND
RESOURCES 112

THE IMPOSSIBILITY OF COMPUTING
ANNUALIZED RATES OF
OCCURRENCE 113

THE PROBLEM WITH “HARD-HEADED
THINKING” 113

PERSPECTIVE 114

Responding to Risk 114

RISK REDUCTION 114

RISK ACCEPTANCE 114

RISK TRANSFERENCE (INSURANCE) 114	ACCOUNTABILITY 127
RISK AVOIDANCE 114	ETHICS 128
2.5 Technical Security Architecture 115	Exception Handling 129
Technical Security Architectures 115	Oversight 130
ARCHITECTURAL DECISIONS 116	POLICIES AND OVERSIGHT 130
DEALING WITH LEGACY SECURITY TECHNOLOGY 116	PROMULGATION 131
Principles 116	ELECTRONIC MONITORING 131
DEFENSE IN DEPTH 116	SECURITY METRICS 131
DEFENSE IN DEPTH VERSUS WEAKEST LINKS 116	AUDITING 132
SINGLE POINTS OF VULNERABILITY 117	ANONYMOUS PROTECTED HOTLINE 132
MINIMIZING SECURITY BURDENS 118	BEHAVIORAL AWARENESS 134
REALISTIC GOALS 118	FRAUD 134
Elements of a Technical Security Architecture 118	SANCTIONS 135
BORDER MANAGEMENT 119	2.7 Governance Frameworks 136
INTERNAL SITE SECURITY MANAGEMENT 119	COSO 137
MANAGEMENT OF REMOTE CONNECTIONS 119	THE COSO FRAMEWORK 137
INTERORGANIZATIONAL SYSTEMS 119	OBJECTIVES 138
CENTRALIZED SECURITY MANAGEMENT 119	REASONABLE ASSURANCE 138
2.6 Policy-Driven Implementation 119	COSO FRAMEWORK COMPONENTS 138
Policies 120	CobIT 139
WHAT ARE POLICIES? 120	THE COBIT FRAMEWORK 140
WHAT, NOT HOW 120	DOMINANCE IN THE UNITED STATES 140
CLARITY 120	The ISO/IEC 27000 Family 141
Categories of Security Policies 121	ISO/IEC 27002 141
CORPORATE SECURITY POLICY 121	ISO/IEC 27001 142
MAJOR POLICIES 121	OTHER 27000 STANDARDS 142
ACCEPTABLE USE POLICY 122	2.8 Conclusion 143
POLICIES FOR SPECIFIC COUNTERMEASURES OR RESOURCES 122	<i>Thought Questions 143</i> •
Policy-Writing Teams 124	<i>Hands-on Projects 143</i> •
Implementation Guidance 124	<i>Project Thought Questions 144</i>
NO GUIDANCE 124	• <i>Case Study 145</i> • <i>Case Discussion Questions 146</i> • <i>Perspective Questions 146</i>
STANDARDS AND GUIDELINES 124	
Types of Implementation Guidance 126	
PROCEDURES 126	
PROCESSES 126	
BASELINES 127	
BEST PRACTICES AND RECOMMENDED PRACTICES 127	
	Chapter 3 Cryptography 147
	3.1 What is Cryptography? 148
	Encryption for Confidentiality 149
	Terminology 149
	PLAINTEXT 149
	ENCRYPTION AND CIPHERTEXT 149
	CIPHER 150
	KEY 150
	KEEPING THE KEY SECRET 150
	The Simple Cipher 150
	Cryptanalysis 151

- Substitution and Transposition
 - Ciphers 152
 - Substitution Ciphers 152
 - Transposition Ciphers 152
 - Real-world Encryption 153
 - Ciphers and Codes 153
 - Symmetric Key Encryption 155
 - KEY LENGTH 155
 - Human Issues in Cryptography 157
- 3.2 Symmetric Key Encryption
 - Ciphers 159
 - RC4 159
 - The Data Encryption Standard (DES) 160
 - 56-BIT KEY SIZE 160
 - BLOCK ENCRYPTION 160
 - Triple DES (3DES) 161
 - 168-BIT 3DES OPERATION 161
 - 112-BIT 3DES 161
 - PERSPECTIVE ON 3DES 162
 - Advanced Encryption Standard (AES) 162
 - Other Symmetric Key Encryption Ciphers 162
- 3.3 Cryptographic System Standards 165
 - Cryptographic Systems 165
 - Initial Handshaking Stages 165
 - NEGOTIATION 165
 - INITIAL AUTHENTICATION 166
 - KEYING 166
 - Ongoing Communication 166
- 3.4 The Negotiation Stage 167
 - Cipher Suite Options 167
 - Cipher Suite Policies 168
- 3.5 Initial Authentication Stage 168
 - Authentication Terminology 168
 - Hashing 169
 - Initial Authentication with MS-CHAP 170
 - ON THE SUPPLICANT'S MACHINE: HASHING 170
 - ON THE VERIFIER SERVER 171

- 3.6 The Keying Stage 172
 - Session Keys 172
 - Public Key Encryption for Confidentiality 172
 - TWO KEYS 172
 - PROCESS 172
 - PADLOCK AND KEY ANALOGY 172
 - HIGH COST AND SHORT MESSAGE LENGTHS 173
 - RSA AND ECC 173
 - KEY LENGTH 174
 - Symmetric Key Keying Using Public Key Encryption 174
 - Symmetric Key Keying Using Diffie–Hellman Key Agreement 175
- 3.7 Message-By-Message Authentication 176
 - Electronic Signatures 176
 - Public Key Encryption for Authentication 176
 - Message-by-Message Authentication with Digital Signatures 177
 - DIGITAL SIGNATURES 177
 - HASHING TO PRODUCE THE MESSAGE DIGEST 177
 - SIGNING THE MESSAGE DIGEST TO PRODUCE THE DIGITAL SIGNATURE 177
 - SENDING THE MESSAGE WITH CONFIDENTIALITY 178
 - VERIFYING THE SUPPLICANT 179
 - MESSAGE INTEGRITY 179
 - PUBLIC KEY ENCRYPTION FOR CONFIDENTIALITY AND AUTHENTICATION 179
 - Digital Certificates 180
 - CERTIFICATE AUTHORITIES 180
 - DIGITAL CERTIFICATE 181
 - VERIFYING THE DIGITAL CERTIFICATE 181
 - THE ROLES OF THE DIGITAL CERTIFICATE AND DIGITAL SIGNATURE 183
 - Key-Hashed Message Authentication Codes 184
 - THE PROBLEM WITH DIGITAL SIGNATURES 184
 - Creating and Testing the HMAC 184
 - Nonrepudiation 186

3.8 Quantum Security	188	3.12 Conclusion	202
3.9 Cryptographic Systems	189	Thought Questions	204 •
Virtual Private Networks (VPNs)	190	Hands-on Projects	205 •
Why VPNs?	190	Project Thought Questions	206
Host-to-Host VPNs	190	• Case Study	207 • Case Discus-
Remote Access VPNs	191	sion Questions	208 • Perspective
Site-to-Site VPNs	191	Questions	208
3.10 SSL/TLS	192	Chapter 4 Secure Networks	209
Nontransparent Protection	192	4.1 Introduction	210
Inexpensive Operation	193	Creating Secure Networks	210
SSL/TLS Gateways and Remote		AVAILABILITY	210
Access VPNs	193	CONFIDENTIALITY	210
VPN GATEWAY STANDARDS	194	FUNCTIONALITY	211
AUTHENTICATION	194	ACCESS CONTROL	211
CONNECTING THE CLIENT PC TO		Future of Secure Networks	211
AUTHORIZED RESOURCES	194	DEATH OF THE PERIMETER	211
SECURITY FOR SERVICES	194	RISE OF THE CITY	212
BROWSER ON THE CLIENT	194	4.2 DoS Attacks	213
ADVANCED SERVICES REQUIRE		Denial of Service ... But Not an	
ADMINISTRATOR PRIVILEGES ON PCs	196	Attack	213
PERSPECTIVE	197	FAULTY CODING	213
3.11 IPsec	197	REFERRALS FROM LARGE SITES	214
Attractions of IPsec	197	Goal of DoS Attacks	214
SSL/TLS GIVES NONTRANSPARENT		STOP CRITICAL SERVICES	214
TRANSPORT LAYER SECURITY	198	DEGRADE SERVICES	214
IPSEC: TRANSPARENT INTERNET LAYER		Methods of DoS Attacks	214
SECURITY	198	DIRECT AND INDIRECT ATTACKS	216
IPSEC IN BOTH IPV4 AND IPV6	198	INTERMEDIARY	218
IPsec Transport Mode	199	REFLECTED ATTACK	220
HOST-TO-HOST SECURITY	199	SENDING MALFORMED PACKETS	221
END-TO-END PROTECTION	199	Defending Against Denial-of-Service	
COST OF SETUP	199	Attacks	222
IPSEC IN TRANSPORT MODE AND		BLACK HOLING	223
FIREWALLS	199	VALIDATING THE HANDSHAKE	224
IPsec Tunnel Mode	200	RATE LIMITING	224
PROTECTION IS PROVIDED BY IPSEC		4.3 ARP Poisoning	225
GATEWAYS	200	Normal ARP Operation	225
LESS EXPENSIVE THAN TRANSPORT		THE PROBLEM	227
MODE	200	ARP Poisoning	227
FIREWALL-FRIENDLY PROTECTION	201	ARP DoS Attack	229
NO PROTECTION WITHIN THE TWO		Preventing ARP Poisoning	229
SITES	201	STATIC TABLES	229
IPsec Security Associations (SAs)	201	LIMIT LOCAL ACCESS	230
SEPARATE SAs IN THE TWO			
DIRECTIONS	201		
POLICY-BASED SA	202		

4.4 Access Control for Networks 232

- LAN Connections 232
- Access Control Threats 232
- Eavesdropping Threats 233

4.5 Ethernet Security 233

- Ethernet and 802.1X 233
 - COST SAVINGS 234
 - CONSISTENCY 234
 - IMMEDIATE CHANGES 234
- The Extensible Authentication Protocol (EAP) 235
 - EAP OPERATION 235
 - EXTENSIBILITY 236
- RADIUS Servers 236
 - RADIUS AND EAP 237

4.6 Wireless Security 237

- Wireless Attacks 238
- Unauthorized Network Access 238
 - PREVENTING UNAUTHORIZED ACCESS 239
- Evil Twin Access Points 241
- Wireless Denial of Service 242
 - FLOOD THE FREQUENCY 242
 - FLOOD THE ACCESS POINT 244
 - SEND ATTACK COMMANDS 244
- Wireless LAN Security with 802.11i 244
 - EAP'S NEED FOR SECURITY 245
 - ADDING SECURITY TO EAP 245
 - EAP-TLS AND PEAP 246
- Core Wireless Security Protocols 247
- Wired Equivalent Privacy (WEP) 247
- Cracking WEP 247
 - SHARED KEYS AND OPERATIONAL SECURITY 247
 - EXPLOITING WEP'S WEAKNESS 248
- Perspective 249
- Wi-Fi Protected Access (WPA™) 249
- Pre-Shared Key (PSK) Mode 252
- Wireless Intrusion Detection Systems 254
- False 802.11 Security Measures 255
 - SPREAD SPECTRUM OPERATION AND SECURITY 255

- TURNING OFF SSID BROADCASTING 255
- MAC ACCESS CONTROL LISTS 255
- Implementing 802.11i or WPA Is Easier 255

4.7 Conclusion 256

- Thought Questions* 258 •
- Hands-on Projects* 258 •
- Project Thought Questions* 259
 - *Case Study* 259
 - *Case Discussion Questions* 261
 - *Perspective Questions* 261

Chapter 5 Access Control 262

5.1 Introduction 263

- Access Control 263
- Authentication, Authorizations, and Auditing 263
- Authentication 264
- Beyond Passwords 264
- Two-Factor Authentication 264
- Individual and Role-Based Access Control 264
- Organizational and Human Controls 266
- Military and National Security Organization Access Controls 266
- Multilevel Security 267

5.2 Physical Access and Security 268

- Risk Analysis 268
- ISO/IEC 9.1: Secure Areas 268
 - PHYSICAL SECURITY PERIMETER 268
 - PHYSICAL ENTRY CONTROLS 268
 - PUBLIC ACCESS, DELIVERY, AND LOADING AREAS 269
 - SECURING OFFICES, ROOMS, AND FACILITIES 269
 - PROTECTING AGAINST EXTERNAL AND ENVIRONMENTAL THREATS 270
 - RULES FOR WORKING IN SECURE AREAS 273
- ISO/IEC 9.2 Equipment Security 273
 - EQUIPMENT SITING AND PROTECTION 273
 - SUPPORTING UTILITIES 274
 - CABLING SECURITY 274

- SECURITY DURING OFF-SITE EQUIPMENT MAINTENANCE 274
- SECURITY OF EQUIPMENT OFF-PREMISES 274
- SECURE DISPOSAL OR REUSE OF EQUIPMENT 274
- REMOVAL OF PROPERTY 274
- Other Physical Security Issues 275**
 - TERRORISM 275
 - PIGGYBACKING 275
 - MONITORING EQUIPMENT 275
 - DUMPSTER™ DIVING 276
 - DESKTOP PC SECURITY 276
 - NOTEBOOK SECURITY 276
- 5.3 Passwords 277**
 - Password-Cracking Programs 277**
 - Password Policies 277**
 - Password Use and Misuse 277**
 - NOT USING THE SAME PASSWORD AT MULTIPLE SITES 278
 - PASSWORD DURATION POLICIES 279
 - POLICIES PROHIBITING SHARED ACCOUNTS 279
 - DISABLING PASSWORDS THAT ARE NO LONGER VALID 279
 - LOST PASSWORDS 280
 - PASSWORD STRENGTH 282
 - PASSWORD AUDITING 282
 - The End of Passwords? 283**
- 5.4 Access Cards and Tokens 284**
 - Access Cards 284**
 - MAGNETIC STRIPE CARDS 285
 - SMART CARDS 285
 - CARD READER COSTS 285
 - Tokens 285**
 - ONE-TIME-PASSWORD TOKENS 286
 - USB TOKENS 286
 - Proximity Access Tokens 286**
 - Addressing Loss and Theft 286**
 - PHYSICAL DEVICE CANCELLATION 286
 - TWO-FACTOR AUTHENTICATION 286
- 5.5 Biometric Authentication 289**
 - Biometrics 289**
 - Biometric Systems 290**
 - INITIAL ENROLLMENT 290
 - SUBSEQUENT ACCESS ATTEMPTS 290
 - ACCEPTANCE OR REJECTION 291
 - Biometric Errors 292**
 - FALSE ACCEPTANCE RATE 292
 - FALSE REJECTION RATE 293
 - WHICH IS WORSE? 293
 - VENDOR CLAIMS 293
 - FAILURE TO ENROLL 293
 - Verification, Identification, and Watch Lists 294**
 - VERIFICATION 294
 - IDENTIFICATION 294
 - WATCH LISTS 295
 - Biometric Deception 296**
 - Biometric Methods 296**
 - FINGERPRINT RECOGNITION 296
 - IRIS RECOGNITION 297
 - FACE RECOGNITION 298
 - HAND GEOMETRY 299
 - VOICE RECOGNITION 303
 - OTHER FORMS OF BIOMETRIC AUTHENTICATION 303
- 5.6 Cryptographic Authentication 303**
 - Key Points from Chapter 3 303**
 - Public Key Infrastructures 304**
 - THE FIRM AS A CERTIFICATE AUTHORITY 304
 - CREATING PUBLIC KEY–PRIVATE KEY PAIRS 304
 - DISTRIBUTING DIGITAL CERTIFICATES 305
 - ACCEPTING DIGITAL CERTIFICATES 305
 - CERTIFICATE REVOCATION STATUS 305
 - PROVISIONING 305
 - THE PRIME AUTHENTICATION PROBLEM 305
- 5.7 Authorization 306**
 - The Principle of Least Permissions 306**
- 5.8 Auditing 308**
 - Logging 308**
 - Log Reading 308**
 - REGULAR LOG READING 308

PERIODIC EXTERNAL AUDITS OF LOG FILE ENTRIES 309
AUTOMATIC ALERTS 309

5.9 Central Authentication Servers 309

The Need for Centralized Authentication 309
Kerberos 310

5.10 Directory Servers 311

What Are Directory Servers? 312
Hierarchical Data Organization 312
Lightweight Data Access Protocol 313
Use by Authentication Servers 313
Active Directory 313
ACTIVE DIRECTORY DOMAINS 313

Trust 315

5.11 Full Identity Management 316

Other Directory Servers and Metadirectories 316
Federated Identity Management 317
THE SECURITY ASSERTION MARKUP LANGUAGE 318
PERSPECTIVE 318

Identity Management 319

BENEFITS OF IDENTITY MANAGEMENT 319
WHAT IS IDENTITY? 319
IDENTITY MANAGEMENT 320

Trust and Risk 321

5.12 Conclusion 322

Thought Questions 324 •
Hands-on Projects 324 •
Project Thought Questions 326
• *Case Study 326 • Case Discussion Questions 327 • Perspective Questions 328*

Chapter 6 Firewalls 329

6.1 Introduction 330

Basic Firewall Operation 330
The Danger of Traffic Overload 334
Firewall Filtering Mechanisms 336

6.2 Static Packet Filtering 336

Looking at Packets One at a Time 337

Looking Only at Some Fields in the Internet and Transport Headers 337

Usefulness of Static Packet Filtering 337

Perspective 339

6.3 Stateful Packet Inspection 339

Basic Operation 339

CONNECTIONS 339
STATES 339
STATEFUL PACKET INSPECTION WITH TWO STATES 340
REPRESENTING CONNECTIONS 341

Packets That Do Not Attempt to Open Connections 341

TCP CONNECTIONS 344
UDP AND ICMP CONNECTIONS 344
ATTACK ATTEMPTS 345
PERSPECTIVE 345

Packets That Do Attempt to Open a Connection 345

Access Control Lists (ACLs) for Connection-Opening Attempts 346

WELL-KNOWN PORT NUMBERS 347
ACCESS CONTROL LISTS (ACLs) FOR INGRESS FILTERING 348
IF-THEN FORMAT 348
PORTS AND SERVER ACCESS 348
DISALLOW ALL CONNECTIONS 349

Perspective on SPI Firewalls 350

LOW COST 350
SAFETY 350
DOMINANCE 350

6.4 Network Address Translation 350

Sniffers 351

NAT OPERATION 351
PACKET CREATION 351
NETWORK AND PORT ADDRESS TRANSLATION (NAT/PAT) 351
TRANSLATION TABLE 351
RESPONSE PACKET 351
RESTORATION 351
PROTECTION 352

Perspective on NAT	352	HOST FIREWALLS	368
NAT/PAT	352	DEFENSE IN DEPTH	369
TRANSPARENCY	352	The Demilitarized Zone (DMZ)	369
NAT TRAVERSAL	352	SECURITY IMPLICATIONS	370
6.5 Application Proxy Firewalls and Content Filtering	352	HOSTS IN THE DMZ	370
Application Proxy Firewall Operation	352	6.9 Firewall Management	371
OPERATIONAL DETAILS	352	Defining Firewall Policies	371
APPLICATION PROXY PROGRAMS VERSUS APPLICATION PROXY FIREWALLS	353	WHY USE POLICIES?	371
PROCESSING-INTENSIVE OPERATION	353	EXAMPLES OF POLICIES	371
ONLY A FEW APPLICATIONS CAN BE PROXIED	353	Implementation	373
TWO COMMON USES	353	FIREWALL HARDENING	373
Application Content Filtering in Stateful Packet Inspection Firewalls	354	CENTRAL FIREWALL MANAGEMENT SYSTEMS	373
Application Content Filtering for HTTP	355	FIREWALL POLICY DATABASE	374
Client Protections	356	VULNERABILITY TESTING AFTER CONFIGURATION	375
Server Protections	357	CHANGE AUTHORIZATION AND MANAGEMENT	375
Other Protections	359	READING FIREWALL LOGS	375
6.6 Intrusion Detection Systems and Intrusion Prevention Systems	360	Reading Firewall Logs	376
Intrusion Detection Systems	360	Log Files	376
FIREWALLS VERSUS IDSs	360	Sorting the Log File by Rule	376
FALSE POSITIVES (FALSE ALARMS)	360	Echo Probes	377
HEAVY PROCESSING REQUIREMENTS	362	External Access to All Internal FTP Servers	378
Intrusion Prevention Systems	362	Attempted Access to Internal Webservers	378
ASICs FOR FASTER PROCESSING	363	Incoming Packet with a Private IP Source Address	378
THE ATTACK IDENTIFICATION CONFIDENCE SPECTRUM	363	Lack of Capacity	378
IPS Actions	363	Perspective	378
DROPPING PACKETS	363	Sizes of Log Files	379
LIMITING TRAFFIC	363	Logging All Packets	379
6.7 Antivirus Filtering and Unified Threat Management	363	6.10 Firewall Filtering Problems	379
6.8 Firewall Architectures	368	The Death of the Perimeter	380
Types of Firewalls	368	AVOIDING THE BORDER FIREWALL	380
MAIN BORDER FIREWALLS	368	EXTENDING THE PERIMETER	381
SCREENING BORDER ROUTERS	368	PERSPECTIVE	381
INTERNAL FIREWALLS	368	Attack Signatures versus Anomaly Detection	381
		ZERO-DAY ATTACKS	382
		ANOMALY DETECTION	382
		ACCURACY	382

6.11 Conclusion 382

- Thought Questions* 384 •
- Hands-on Projects* 385 •
- Project Thought Questions* 387
 - *Case Study* 387
 - *Case Discussion Questions* 389
 - *Perspective Questions* 389

Chapter 7 Host Hardening 390

7.1 Introduction 391

- What Is a Host? 391
- The Elements of Host Hardening 391
- Security Baselines and Images 392
- Virtualization 393
 - VIRTUALIZATION ANALOGY 394
 - BENEFITS OF VIRTUALIZATION 395
- Systems Administrators 395

7.2 Important Server Operating Systems 401

- Windows Server Operating Systems 401
 - THE WINDOWS SERVER USER INTERFACE 401
 - START → ADMINISTRATIVE TOOLS 402
 - MICROSOFT MANAGEMENT CONSOLES (MMCs) 402
- UNIX (Including Linux) Servers 403
 - MANY VERSIONS 404
 - LINUX 405
 - UNIX USER INTERFACES 406

7.3 Vulnerabilities and Patches 407

- Vulnerabilities and Exploits 407
- Fixes 407
 - WORK-AROUNDS 411
 - PATCHES 411
 - SERVICE PACKS 412
 - VERSION UPGRADES 412

The Mechanics of Patch Installation 412

- MICROSOFT WINDOWS SERVER 412
- LINUX RPM PROGRAM 412

Problems with Patching 412

- THE NUMBER OF PATCHES 412
- COST OF PATCH INSTALLATION 413

- PRIORITIZING PATCHES 413
- PATCH MANAGEMENT SERVERS 413
- THE RISKS OF PATCH INSTALLATION 414

7.4 Managing Users and Groups 414

The Importance of Groups in Security Management 414

Creating and Managing Users and Groups in Windows 415

- THE ADMINISTRATOR ACCOUNT 415
- MANAGING ACCOUNTS 415
- CREATING USERS 416
- WINDOWS GROUPS 416

7.5 Managing Permissions 417

Permissions 417

Assigning Permissions in Windows 418

- DIRECTORY PERMISSIONS 418
- WINDOWS PERMISSIONS 419
- ADDING USERS AND GROUPS 419
- INHERITANCE 419
- DIRECTORY ORGANIZATION 419

Assigning Groups and Permissions in UNIX 420

- NUMBER OF PERMISSIONS 421
- NUMBER OF ACCOUNTS OR GROUPS 421

7.6 Creating Strong Passwords 421

Creating and Storing Passwords 422

- CREATING A PASSWORD HASH 422
- STORING PASSWORDS 422
- STEALING PASSWORDS 423

Password-Cracking Techniques 423

- BRUTE-FORCE GUESSING 423
- DICTIONARY ATTACKS ON COMMON WORD PASSWORDS 425
- HYBRID DICTIONARY ATTACKS 426
- RAINBOW TABLES 427
- TRULY RANDOM PASSWORDS 427
- TESTING AND ENFORCING THE STRENGTH OF PASSWORDS 428
- OTHER PASSWORD THREATS 428

7.7 Testing For Vulnerabilities 429

Windows Client PC Security 430

Client PC Security Baselines 430

The Windows Action Center 430

Windows Firewall	431	MINIMIZE APPLICATIONS	451
Automatic Updates	432	SECURITY BASELINES FOR APPLICATION MINIMIZATION	452
Antivirus and Spyware Protection	433	CREATE A SECURE CONFIGURATION	452
Implementing Security Policy	434	INSTALL APPLICATION PATCHES AND UPDATES	453
PASSWORD POLICIES	434	MINIMIZE THE PERMISSIONS OF APPLICATIONS	453
ACCOUNT POLICIES	434	ADD APPLICATION-LEVEL AUTHENTICATION, AUTHORIZATIONS, AND AUDITING	453
AUDIT POLICIES	434	IMPLEMENT CRYPTOGRAPHIC SYSTEMS	453
Protecting Notebook Computers	436	Securing Custom Applications	453
THREATS	436	NEVER TRUST USER INPUT	454
BACKUP	436	BUFFER OVERFLOW ATTACKS	454
POLICIES FOR SENSITIVE DATA	437	LOGIN SCREEN BYPASS ATTACKS	455
TRAINING	437	CROSS-SITE SCRIPTING ATTACKS	455
COMPUTER RECOVERY SOFTWARE	437	SQL INJECTION ATTACKS	455
Centralized PC Security		AJAX MANIPULATION	456
Management	437	TRAINING IN SECURE COMPUTING	456
STANDARD CONFIGURATIONS	438	8.2 WWW and E-Commerce Security	459
NETWORK ACCESS CONTROL	438	The Importance of WWW and E-Commerce Security	459
WINDOWS GROUP POLICY OBJECTS	438	WWW Service versus E-Commerce Service	459
7.8 Conclusion	441	WWW SERVICE	459
<i>Thought Questions</i>	442	E-COMMERCE SERVICE	459
• <i>Hands-on Projects</i>	442	EXTERNAL ACCESS	460
• <i>Project Thought Questions</i>	443	CUSTOM PROGRAMS	461
• <i>Case Study</i>	443	Some Webserver Attacks	461
• <i>Case Discussion Questions</i>	445	WEBSITE DEFAACEMENT	461
• <i>Perspective Questions</i>	445	BUFFER OVERFLOW ATTACK TO LAUNCH A COMMAND SHELL	462
Chapter 8 Application Security	446	DIRECTORY TRAVERSAL ATTACK	462
8.1 Application Security and Hardening	447	THE DIRECTORY TRAVERSAL WITH HEXADECIMAL CHARACTER ESCAPES	462
Executing Commands with the Privileges of a Compromised Application	447	UNICODE DIRECTORY TRAVERSAL	463
Buffer Overflow Attacks	447	Patching the Webserver and E-Commerce Software and Its Components	463
BUFFERS AND OVERFLOWS	448	E-COMMERCE SOFTWARE VULNERABILITIES	463
STACKS	448	Other Website Protections	464
RETURN ADDRESS	448	WEBSITE VULNERABILITY ASSESSMENT TOOLS	464
THE BUFFER AND BUFFER OVERFLOW	448		
EXECUTING ATTACK CODE	448		
AN EXAMPLE: THE IIS IPP BUFFER OVERFLOW ATTACK	449		
Few Operating Systems, Many Applications	449		
Hardening Applications	450		
UNDERSTAND THE SERVER'S ROLE AND THREAT ENVIRONMENT	450		
THE BASICS	451		

- WEBSITE ERROR LOGS 464
- WEBSERVER-SPECIFIC APPLICATION PROXY FIREWALLS 465
- Controlling Deployment 465**
 - DEVELOPMENT SERVERS 465
 - TESTING SERVERS 465
 - PRODUCTION SERVERS 465
- 8.3 Web Browser Attacks 466**
 - BROWSER THREATS 466
 - MOBILE CODE 466
 - MALICIOUS LINKS 468
 - OTHER CLIENT-SIDE ATTACKS 468
- Enhancing Browser Security 470**
 - PATCHING AND UPGRADING 470
 - CONFIGURATION 470
 - INTERNET OPTIONS 470
 - SECURITY TAB 470
 - PRIVACY TAB 474
- 8.4 E-Mail Security 475**
 - E-Mail Content Filtering 475**
 - MALICIOUS CODE IN ATTACHMENTS AND HTML BODIES 475
 - SPAM 475
 - INAPPROPRIATE CONTENT 476
 - EXTRUSION PREVENTION 476
 - PERSONALLY IDENTIFIABLE INFORMATION 476
 - Where to Do E-Mail Malware and Spam Filtering 477**
 - E-Mail Encryption 478**
 - TRANSMISSION ENCRYPTION 478
 - MESSAGE ENCRYPTION 478
- 8.5 Voice over IP Security 480**
 - Sending Voice between Phones 480**
 - Transport and Signaling 481
 - SIP and H.323 481
 - Registration 481
 - SIP Proxy Servers 481
 - PSTN Gateway 482
 - VoIP Threats 482
 - Eavesdropping 482
 - Denial-of-Service Attacks 483
 - Caller Impersonation 483
 - Hacking and Malware Attacks 483

- Toll Fraud 484
- Spam over IP Telephony 484
- New Threats 484
- Implementing VoIP Security 485
- Authentication 485
- Encryption for Confidentiality 486
- Firewalls 486
- NAT Problems 486
- Separation: Anticonvergence 486
- The Skype VoIP Service 487
- 8.6 Other User Applications 488**
 - Instant Messaging 488
 - TCP/IP Supervisory Applications 490
- 8.7 Conclusion 491**
 - Thought Questions 492 • Hands-on Projects 492 • Project Thought Questions 494 • Case Study 494 • Case Discussion Questions 495 • Perspective Questions 495*

Chapter 9 Data Protection 496

- 9.1 Introduction 497**
 - Data's Role in Business 497
 - SONY DATA BREACHES 497
 - Securing Data 498
- 9.2 Data Protection: Backup 498**
 - The Importance of Backup 498
 - Threats 498
 - Scope of Backup 498
 - FILE/DIRECTORY DATA BACKUP 499
 - IMAGE BACKUP 499
 - SHADOWING 499
 - Full versus Incremental Backups 501
 - Backup Technologies 502
 - LOCAL BACKUP 502
 - CENTRALIZED BACKUP 504
 - CONTINUOUS DATA PROTECTION 504
 - INTERNET BACKUP SERVICE 505
 - MESH BACKUP 505
- 9.3 Backup Media and Raid 506**
 - MAGNETIC TAPE 506
 - CLIENT PC BACKUP 507

Disk Arrays—RAID	507		
Raid Levels	508		
No RAID	508		
RAID 0	509		
RAID 1	509		
RAID 5	511		
9.4 Data Storage Policies	514		
Backup Creation Policies	514		
Restoration Policies	514		
Media Storage Location Policies	514		
Encryption Policies	515		
Access Control Policies	515		
Retention Policies	516		
Auditing Backup Policy Compliance	516		
E-Mail Retention	516		
The Benefit of Retention	516		
The Dangers of Retention	516		
Accidental Retention	517		
Third-Party E-mail Retention	517		
Legal Archiving Requirements	517		
U.S. Federal Rules of Civil Procedure	517		
Message Authentication	519		
Developing Policies and Processes	519		
User Training	519		
Spreadsheets	520		
Vault Server Access Control	520		
Other Vault Server Protections	521		
9.5 Database Security	521		
Relational Databases	522		
Limiting the View of Data	522		
Database Access Control	526		
Database Accounts	526		
SQL Injection Attacks	526		
Database Auditing	527		
What to Audit	527		
Triggers	528		
Database Placement and Configuration	529		
Change the Default Port	530		
Data Encryption	530		
Key Escrow	530		
File/Directory Encryption Versus Whole-Disk Encryption	532		
			Protecting Access to the Computer 532
			Difficulties in File Sharing 532
9.6 Data Loss Prevention	532		
Data Collection	532		
Personally Identifiable Information	533		
Data Masking	533		
Information Triangulation	535		
Buy or Sell Data	536		
Document Restrictions	537		
Digital Rights Management	537		
Data Extrusion Management	538		
Extrusion Prevention	538		
Data Loss Prevention Systems	538		
DLP at the Gateway	540		
DLP on Clients	540		
DLP for Data Storage	540		
DLP Manager	540		
Watermarks	540		
Removable Media Controls	541		
Perspective	542		
Employee Training	542		
Social Networking	542		
Data Destruction	543		
Nominal Deletion	543		
Basic File Deletion	544		
Wiping/Clearing	545		
Destruction	545		
9.7 Conclusion	546		
			<i>Thought Questions</i> 546 •
			<i>Hands-on Projects</i> 547 •
			<i>Project Thought Questions</i> 548
			• <i>Case Study</i> 548 • <i>Case Discussion Questions</i> 550 • <i>Perspective Questions</i> 550
Chapter 10 Incident and Disaster Response 551			
10.1 Introduction	552		
Walmart and Hurricane Katrina	552		
Incidents Happen	553		
Incident Severity	553		
False Alarms	553		
Minor Incidents	553		
Major Incidents	553		
Disasters	555		

Speed and Accuracy 556

- SPEED IS OF THE ESSENCE 556
- SO IS ACCURACY 556
- PLANNING 557
- REHEARSAL 557

10.2 The Intrusion Response Process For Major Incidents 558

Detection, Analysis, and Escalation 558

- DETECTION 558
- ANALYSIS 560
- ESCALATION 560

Containment 560

- DISCONNECTION 560
- BLACK-HOLING THE ATTACKER 560
- CONTINUING TO COLLECT DATA 560

Recovery 561

- REPAIR DURING CONTINUING SERVER OPERATION 561
- RESTORATION FROM BACKUP TAPES 561
- TOTAL SOFTWARE REINSTALLATION 562

Apology 562

Punishment 562

- PUNISHING EMPLOYEES 562
- THE DECISION TO PURSUE PROSECUTION 563
- COLLECTING AND MANAGING EVIDENCE 563

Postmortem Evaluation 565

Organization of the CSIRT 565

Legal Considerations 566

Criminal versus Civil Law 566

Jurisdictions 567

The U.S. Federal Judicial System 568

U.S. State and Local Laws 568

International Law 569

Evidence and Computer Forensics 571

U.S. Federal Cybercrime Laws 572

- COMPUTER HACKING, MALWARE ATTACKS, DENIAL-OF-SERVICE ATTACKS, AND OTHER ATTACKS (18 U.S.C. § 1030) 572
- HACKING 573

- DENIAL-OF-SERVICE AND MALWARE ATTACKS 573
- DAMAGE THRESHOLDS 573

Confidentiality in Message Transmission 574

Other Federal Laws 574

10.3 Intrusion Detection Systems 574

Functions of an IDS 575

- LOGGING (DATA COLLECTION) 575
- AUTOMATED ANALYSIS BY THE IDS 576
- ACTIONS 576
- LOG SUMMARY REPORTS 576
- SUPPORT FOR INTERACTIVE MANUAL LOG ANALYSIS 576

Distributed IDSs 577

- AGENTS 577
- MANAGER AND INTEGRATED LOG FILE 577
- BATCH VERSUS REAL-TIME DATA TRANSFER 577
- SECURE MANAGER-AGENT COMMUNICATION 578
- VENDOR COMMUNICATION 578

Network IDSs 578

- STAND-ALONE NIDSs 578
- SWITCH AND ROUTER NIDSs 578
- STRENGTHS OF NIDSs 578
- WEAKNESSES OF NIDSs 578
- HOST IDSs 579
- ATTRACTION OF HIDSs 579
- WEAKNESSES OF HOST IDSs 580
- HOST IDSs: OPERATING SYSTEM MONITORS 580

Log Files 580

- TIME-STAMPED EVENTS 580
- INDIVIDUAL LOGS 580
- INTEGRATED LOGS 580
- MANUAL ANALYSIS 582

Managing IDSs 583

- TUNING FOR PRECISION 583

Honey pots 584

10.4 Business Continuity Planning 589

Principles of Business Continuity Management 591

- PEOPLE FIRST 591
- REDUCED CAPACITY IN DECISION MAKING 591
- AVOIDING RIGIDITY 591

COMMUNICATION, COMMUNICATION, COMMUNICATION	591		
Business Process Analysis	592		
IDENTIFICATION OF BUSINESS PROCESSES AND THEIR INTERRELATIONSHIPS	592		
PRIORITIZATION OF BUSINESS PROCESSES	592		
SPECIFY RESOURCE NEEDS	592		
SPECIFY ACTIONS AND SEQUENCES	592		
Testing and Updating the Plan	592		
10.5 IT Disaster Recovery	593		
Types of Backup Facilities	594		
HOT SITES	594		
COLD SITES	594		
SITE SHARING WITH CONTINUOUS DATA PROTECTION	594		
LOCATION OF THE SITES	595		
Office PCs	598		
DATA BACKUP	598		
NEW COMPUTERS	598		
WORK ENVIRONMENT	598		
Restoration of Data and Programs	598		
Testing the IT Disaster Recovery Plan	599		
10.6 Conclusion	599		
<i>Thought Questions</i>	600	•	
<i>Hands-on Projects</i>	600	•	
<i>Project Thought Questions</i>	601		
• <i>Case Study</i>	601	•	<i>Case Discus-</i>
• <i>Discussion Questions</i>	603	•	<i>Perspective</i>
• <i>Questions</i>	603		
Module A Networking Concepts	604		
A.1 Introduction	604		
A.2 A Sampling of Networks	605		
A Simple Home Network	605		
THE ACCESS ROUTER	605		
PERSONAL COMPUTERS	606		
UTP WIRING	606		
INTERNET ACCESS LINE	607		
A Building LAN	607		
A Firm's Wide Area Networks	608		
The Internet	610		
Applications	612		
A.3 Network Protocols and Vulnerabilities	613		
			Inherent Security 613
			Security Explicitly Designed into the Standard 613
			Security in Older Versions of the Standard 613
			Defective Implementation 614
			A.4 Core Layers in Layered Standards Architectures 614
			A.5 Standards Architectures 615
			The TCP/IP Standards Architecture 615
			The OSI Standards Architecture 616
			The Hybrid TCP/IP-OSI Architecture 616
			A.6 Single-Network Standards 616
			The Data Link Layer 617
			The Physical Layer 617
			UTP 617
			OPTICAL FIBER 617
			WIRELESS TRANSMISSION 618
			SWITCH SUPERVISORY FRAMES 618
			A.7 Internetworking Standards 619
			A.8 The Internet Protocol 620
			The IP Version 4 Packet 620
			The First Row 620
			The Second Row 621
			The Third Row 621
			Options 622
			The Source and Destination IP Addresses 622
			Masks 622
			IP Version 6 623
			IPsec 624
			A.9 The Transmission Control Protocol 625
			TCP: A Connection-Oriented and Reliable Protocol 625
			CONNECTIONLESS AND CONNECTION- ORIENTED PROTOCOLS 625
			RELIABILITY 627
			Flag Fields 628
			Sequence Number Field 628
			Acknowledgment Number Field 629

Window Field	629	Simple Network Management Protocol	638
Options	630	A.12 Application Standards	639
Port Numbers	630	HTTP AND HTML	639
PORT NUMBERS ON SERVERS	630	E-MAIL	640
PORT NUMBERS ON CLIENTS	631	TELNET, FTP, AND SSH	641
SOCKETS	631	OTHER APPLICATION STANDARDS	641
TCP Security	632	A.13 Conclusion	641
A.10 The User Datagram Protocol	632	<i>Hands-on Projects</i>	641 •
A.11 TCP/IP Supervisory Standard	634	<i>Project Thought Questions</i>	643 •
Internet Control Message Protocol	634	<i>Perspective Questions</i>	643
The Domain Name System	635	Glossary	644
Dynamic Host Configuration Protocol	636	Index	661
Dynamic Routing Protocols	637		

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.

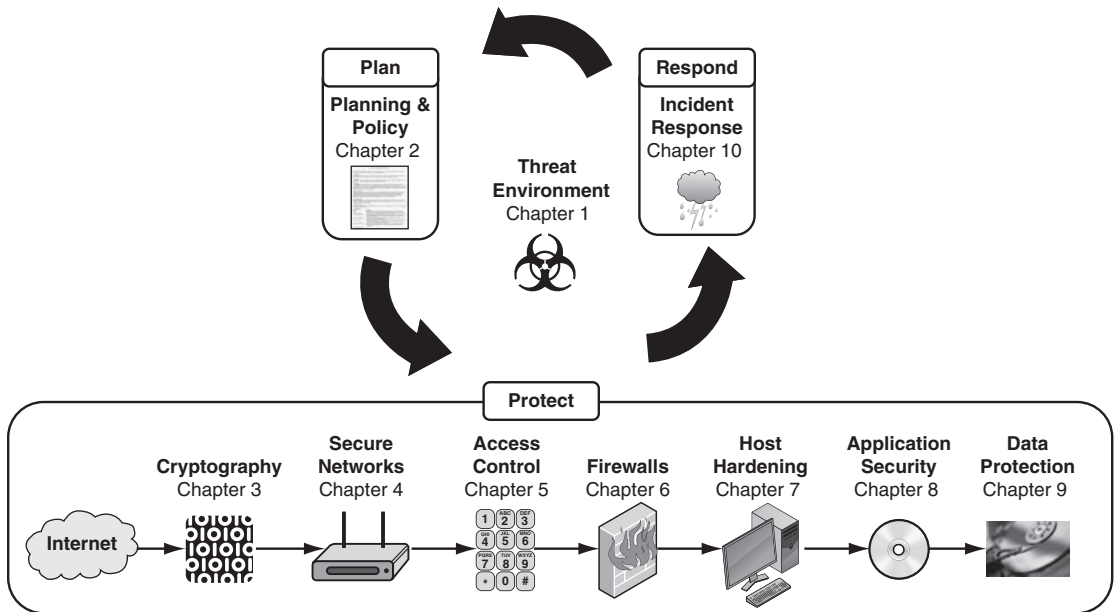
BALANCING TECHNICAL AND MANAGERIAL CONTENT Our students are going to need jobs. When you ask working IT security professionals what they are looking for in a new hire, they give similar responses. They want proactive workers who can take initiative, learn on their own, have strong technical skills, and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

The publishers would like to thank the following for their contribution to the Global Edition:

Contributor

Sahil Raj, Punjabi University

Reviewers

Fabian Ng Yaw Tong, School of InfoComm Technology, Ngee Ann Polytechnic

Lucas Chi Kwong HUI, The University of Hong Kong

Ng Hu, Multimedia University

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 is 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/#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/>.