## CONTENTS

**Preface** xxiii

### Chapter 1  The Threat Environment: Attackers and their Attacks  1

**Introduction** 1
- Basic Security Terminology 1
- The TJX Data Breach 4

**Employee and Ex-Employee Threats** 9
- Why Employees Are Dangerous 9
- Employee Sabotage 9
- Employee Hacking 11
- Employee Financial Theft and Theft of Intellectual Property (IP) 12
- Employee Extortion 13
- Employee Sexual or Racial Harassment 14
- Employee Computer and Internet Abuse 14
- Data Loss 15
- Other “Internal” Attackers 15

**Traditional External Attackers I:**
- Malware Writers 16
- Malware Writers 16
- Viruses 17
- Worms 18
- Blended Threats 19
- Payloads 19
- Trojan Horses and Rootkits 20
- Mobile Code 23
- Social Engineering in Malware 23

**Traditional External Attackers II:** Hackers and Denial-of-Service Attacks 25
- Traditional Motives 25
- Anatomy of a Hack 27
- Social Engineering 30
- Denial-of-Service (DoS) Attacks 31
- Skill Levels 33
Chapter 2 Planning 51

Introduction 51
Defense 51
Management Processes 52
The Need for a Disciplined Security Management Process 54
The Plan–Protect–Respond Cycle 55
Vision in Planning 57
Strategic IT Security Planning 59
BOX: Compliance Laws and Regulations 61

Organization 65
Chief Security Officers (CSOs) 65
Should You Place Security within IT? 65
Top Management Support 67
Relationships with Other Departments 68
Outsourcing IT Security 69

Risk Analysis 72
Reasonable Risk 72
Classic Risk Analysis Calculations 73
Problems with Classic Risk Analysis Calculations 74
Responding to Risk 77
Chapter 3  The Elements of Cryptography  107

What Is Cryptography?  108

Encryption for Confidentiality  108

Terminology  108

The Simple Cipher  110

Cryptanalysis  111

- BOX: Substitution and Transposition Ciphers  111
- BOX: Ciphers and Codes  113

Symmetric Key Encryption  114

Human Issues in Cryptography  116

Symmetric Key Encryption Ciphers  117

RC4  117

The Data Encryption Standard (DES)  118

Triple DES (3DES)  119

Advanced Encryption Standard (AES)  120

Other Symmetric Key Encryption Ciphers  120

Cryptographic Systems  121

Cryptographic Systems  121
Chapter 4 Cryptographic System Standards 149

Introduction 149

Virtual Private Networks (VPNs) 151

Why VPNs? 151

Host-to-Host VPNs 151
Chapter 5  Access Control  193

Introduction  193
  Access Control  193
  Authentication, Authorizations, and Auditing  194
  Authentication  195
  Beyond Passwords  195
  Two-Factor Authentication  195
  Individual and Role-Based Access Control  196

Organizational and Human Controls  196
  BOX: Military and National Security Organization Access Controls  197

Physical Access and Security  198
  Risk Analysis  198
  ISO/IEC 9.1: Secure Areas  198
  9.2 Equipment Security  201
  Other Physical Security Issues  202

Reusable Passwords  204
  Password-Cracking Programs  205
  Password Cracking Techniques  206
  Password Policies  208
  Other Password Policies  210
  The End of Passwords?  213

Access Cards and Tokens  213
  Access Cards  214
  Tokens  215
  Proximity Access Tokens  215
  Addressing Loss and Theft  216

Biometric Authentication  217
  Biometrics  217
  Biometric Systems  218
  Biometric Errors  219
  Verification, Identification, and Watch Lists  221
  Biometric Deception  223
  Biometric Methods  225

Cryptographic Authentication  227
  Key Points from Chapters 3  227
  Public Key Infrastructures (PKIs)  227
Chapter 6  Firewalls  251

Introduction 251
   Basic Firewall Operation 251
   The Danger of Traffic Overload 253
   Firewall Filtering Mechanisms 254

Static Packet Filtering 255
   Looking at Packets One at a Time 255
   Looking Only at Some Fields in the Internet and Transport Headers 255
   Usefulness of Static Packet Filtering 255
   Perspective 257

Stateful Packet Inspection (SPI) 258
   Basic Operation 258
   Packets that Do Not Attempt to Open Connections 260
Packets that Do Attempt to Open a Connection 262
Access Control Lists (ACLs) for Connection-Opening Attempts 262
Perspective on SPI Firewalls 266
Network Address Translation (NAT) 267
Sniffers 267
NAT Operation 267
Perspective on NAT 268
Application Proxy Firewalls and Application Content Filtering 269
Application Proxy Firewall Operation 269
Application Content Filtering in Stateful Packet Inspection Firewalls 271
  ▪ BOX: Application Proxy Firewall Protections 272
Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) 274
Intrusion Detection Systems (IDSs) 274
Intrusion Prevention Systems (IPSs) 277
IPS Actions 278
Antivirus Filtering and Unified Threat Management (UTM) 278
  ▪ BOX: Denial-of-Service (DoS) Protection 280
Firewall Architectures 281
Types of Firewalls 281
The Demilitarized Zone (DMZ) 282
Firewall Management 284
  Defining Firewall Policies 284
Implementation 286
  ▪ BOX: Reading Firewall Logs 290
Difficult Problems for Firewall Filtering 293
The Death of the Perimeter 293
Attack Signatures versus Anomaly Detection 295
Conclusion 296
Synopsis 296
  Thought Questions 298  •  Design Question 299  •  Troubleshooting Question 299  •  Perspective Questions 299

Chapter 7 Host and Data Security 301
Introduction 301
What Is a Host? 301
The Elements of Host Hardening 302
Contents xvii

Security Baselines and Image 303
Systems Administrators 304

Important Server Operating Systems 304
Windows Server Operating Systems 305
UNIX (Including LINUX) Servers 307

Vulnerabilities and Patches 310
Vulnerabilities and Exploits 310
Fixes 311
The Mechanics of Patch Installation 312
Problems with Patching 313

Managing Users and Groups 314
The Importance of Groups in Security Management 314
Creating and Managing Users and Groups in Windows 315

Managing Permissions 318
Permissions 318
Assigning Permissions in Windows 319
Assigning Groups and Permissions in UNIX 321

Testing for Vulnerabilities 322

Windows Client PC Security 323
Client PC Security Baselines 323
The Windows Security Center 324
Automatic Updates 324

Antivirus and Spyware Protection 325
Windows Firewall 326

Protecting Notebook Computers 326

Centralized PC Security Management 328

Data Protection: Backup 331
The Importance of Backup 331
Threats 331
Scope of Backup 332
Full versus Incremental Backups 333
Backup Technologies 335
Backup Media 337
Backup Management Policies 339

Other Data Protections 341
Encryption 341
Data Destruction 343
Chapter 8  Application Security  349

General Application Security Issues  349
  Executing Commands with the Privileges
  of a Compromised Application  349
Buffer Overflow Attacks  350
Few Operating Systems, Many Applications  352
Hardening Applications  352
Securing Custom Applications  355
WWW and E-Commerce Security  358
  The Importance of WWW and E-Commerce Security  358
WWW Service versus E-Commerce Service  358
Some Webserver Attacks  360
Patching the Webserver and E-Commerce Software
  and Its Components  362
Other Website Protections  363
Controlling Deployment  363
Browser Attacks  364
Enhancing Browser Security  367

E-Mail Security  369
  E-Mail Content Filtering  369
Where to Do E-Mail Malware and Spam Filtering  371
E-Mail Retention  372
User Training  375
E-Mail Encryption  376
  • BOX: Voice over IP (VoIP) Security  377
  • BOX: The Skype VoIP Service  384

Other User Applications  385
  Database  385
  Instant Messaging (IM)  386
  Spreadsheets  386

TCP/IP Supervisory Applications  388

Conclusion  390
  Thought Questions  390
  Troubleshooting Questions  391
  Perspective Questions  391
Chapter 9 Incident and Disaster Response 393

Introduction 393

Wal-Mart and Hurricane Katrina 393

Incidents Happen 395

Incident Severity 395

Speed and Accuracy 398

The Intrusion Response Process for Major Incidents 400

Detection, Analysis, and Escalation 401

Containment 402

Recovery 403

Apology 404

Punishment 404

Postmortem Evaluation 407

Organization of the CSIRT 407

• BOX: Legal Considerations 408

Intrusion Detection Systems (IDSs) 415

Functions of an IDS 416

Distributed IDSs 418

Network IDSs (NIDSs) 419

Host IDSs 421

Log Files 422

Managing IDSs 424

Honeypots 426

Business Continuity Planning 426

Principles of Business Continuity Management 428

Business Process Analysis 430

Testing and Updating the Plan 430

IT Disaster Recovery 431

Types of Backup Facilities 432

Office PCs 434

Restoration of Data and Programs 434

Testing the IT Disaster Recovery Plan 435

Conclusion 435

Synopsis 435

Thought Questions 436 • Troubleshooting Question 436 • Perspective Questions 436
MODULE A Networking Concepts 437

Introduction 437

A Sampling of Networks 438
  A Simple Home Network 438
  A Building LAN 440
  A Firm’s Wide Area Networks (WANs) 442
The Internet 443
Applications 446

Network Protocols and Vulnerabilities 446
  Inherent Security 446
  Security Explicitly Designed into the Standard 447
  Security in Older Versions of the Standard 447
  Defective Implementation 447

Core Layers in Layered Standards Architecture 447

Standards Architectures 448
  The TCP/IP Standards Architecture 448
  The OSI Standards Architecture 449
  The Hybrid TCP/IP-OSI Architecture 449

Single-Network Standards 450
  The Data Link Layer 450
  The Physical Layer 451

Internetworking Standards 452
The Internet Protocol (IP) 453
  The IP Version 4 Packet 453
    The First Row 454
    The Second Row 454
    The Third Row 455
    Options 455
    The Source and Destination IP Addresses 456
    Masks 456
    IP Version 6 457
    IPsec 458

The Transmission Control Protocol (TCP) 458
  TCP: A Connection-Oriented and Reliable Protocol 459
    Flag Fields 462
    Sequence Number Field 462
    Acknowledgment Number Field 463
Window Field  463
Options  464
Port Numbers  464
TCP Security  466
The User Datagram Protocol  467
TCP/IP Supervisory Standards  468
  Internet Control Message Protocol (ICMP)  468
  The Domain Name System (DNS)  469
  Dynamic Host Configuration Protocol (DHCP)  471
  Dynamic Routing Protocols  471
  Simple Network Management Protocol (SNMP)  473
Application Standards  473
Conclusion  475

Glossary  477

Index  491