



International
Edition

The Management of Network Security

TECHNOLOGY, DESIGN, AND MANAGEMENT CONTROL

Houston H. Carr
Charles A. Snyder
Bliss N. Bailey

PEARSON

CONTENTS

Preface xvii

Introduction Why Do We Need Security? 1

Introduction 1

Networks and Their Value 4

Network Security 6

Total Security Thinking 6

The Forms of Risk 7

Forms of Protection 9

Achieving Organizational Security 9

PART I Security Fundamentals 11

Chapter 1 Security Is the Result of Risk Assessment and Management 13

Introduction 13

The Nature of Security 14

Network Security 14

Forms of Security 15

The Nature of Risk 16

Who Did It Right? 19

Risk Assessment, Analysis, and Management 20

Risk Management 20

Risk versus Uncertainty 20

Risk Assessment 22

Risk Identification, Measurement, and Treatment 23

A Model for Risk Management 24

Contingency Planning 25

Disaster Planning 26

Data (Information) Security 26

CIA Model of Data Characteristics 27

The CAIN Model of Information Security 28

Backup Copies of Data 29

Metadata 29

What the Organization Must Do 29

*Chapter Summary 31 • Key Terms 31 • Review Questions 31 •
Vital Organizational Management Issues 32 • Vital Organizational
Technical Issues 32 • Projects and Exercises 32 •*

Chapter 2 Properties of a Good Network Environment 35

Introduction 35

Characteristics of a Valuable Network 35

Electric Power for Network Equipment 37

Characteristics of Good Electric Power 37

Providing Continuous Reliable Power 38

The Wires to Watch Out For 40

Power over Ethernet 41

Battery Life 42

What We Can Protect 43

Internal versus External Circuits 43

Protection of Circuits 45

Network Grounding 47

Why Electric Grounding Is Important 47

Lightning 49

Where Lightning Is the Worst 50

Solar Flares (Also Known as "Sunspots") 50

Physical Security of Equipment 52

Providing Physical Security 56

Acts of God (Also Known as "Nature")

versus Acts of Humans 56

Chapter Summary 57 • Key Terms 58 • Review Questions 58 • Vital Organizational Management Issues 59 • Vital Organizational Technology Issues 59 • Projects and Exercises 59 • Case 2-1 Protection from the Pending Storm 60 • Lab Exercise 2-1 Physical Security Risk Assessment 60

Chapter 3 Computer Security Fundamentals 61

Introduction 61

Essentials of a Network Security Model 61

Prevention Tactics 62

Architecture 62

Authentication 64

Authorization 69

Accountability 70

Detection Tactics 70

Correction Tactics 71

Security Layers: Defense in Depth 72

Perimeter Layer Security	74
Area Layer Security	75
Network Access Control	76
Hardware Layer Security	78
Data Layer Security	79
Broad Categories of Threats	80
Random Threats	80
Focused Threats	81
Attackers	82
<i>Chapter Summary 83 • Key Terms 84 • Review Questions 84 •</i> <i>Vital Organizational Management Issues 85 • Vital Organizational</i> <i>Technology Issues 85 • Projects and Exercises 85 • Case 3-1</i> <i>Architecture and Authentication 86 • Lab Exercise 3-1 Authentication</i> <i>and Authorization 86</i>	

PART II The Threats 87

Chapter 4 Threats to Network Security 89

Introduction	89
Broad Categories of Threats	90
Threats versus Effect	90
Random Threats	92
Systems Software Vulnerabilities	92
Environmental Hazards	93
Crosstalk	93
Unreliable Electric Power	94
Ground Loops	94
Damage to Circuits	94
Malware, Grayware, and Weatherbug	95
Grayware	97
Weatherbug	99
Unintentional Acts	100
Focused Threats	101
Email Spam	101
Spoofing	104
Browser and System Hijacking	105
Botnets	106
Port Scanning	107
Denial-of-Service Attack	109
Intrusion	109

Social Engineering	110
Online Gaming Social Engineering	111
Disgruntled Employees	112
Voice (and Video) over Internet Protocol (VoIP)	112
Threats to VoIP	113
The Attackers	113

The Best Defense Is a Strong Offense: Training 113

Chapter Summary 113 • Key Terms 114 • Review Questions 114
• Vital Organizational Management Issues 114 • Vital Organizational
Technology Issues 115 • Projects and Exercises 115 • Lab Exercise
4-1 Securing the Windows Workstation 115 • Lab Exercise 4-2 Ping
Attack DoS 116 • Case 4-1 Threats to Business Continuity 116 •
Case 4-2 Finding the Threats 116 • Appendix 4-1 Examples of
Phishing Emails 117

Chapter 5 Techniques and Technology for Security Management 135

Introduction 135

Prevention: Reaction to Threats 135

Static Threats	136
Software Vulnerabilities	137
Crosstalk	137
Wireless Crosstalk	137
Wired Crosstalk	138
Unreliable Electric Power	139
Dynamic Threats	139
Malware and Grayware	139
Email Spam	141
Blacklist	141
Heuristics	142
Bayesian Filter	142
Filters versus Blacklists	143
Phishing Spam Email	144
Phishing Web Site Filter	145
Social Engineering	146
Intrusion	147

Perimeter Security Measures 147

Border Routers	148
Firewalls	148
Firewall Technologies	149
Personal Firewalls	151
Demilitarized Zone	152

Intrusion Detection Systems: After-the-fact Detection	152
IDS Methodologies	154
Intrusion Prevention Systems	154
Honeypots	155
Sniffers	156
IDS/IPS Approaches	157
Encryption	158
Conclusion	158

<i>Chapter Summary</i>	158	•	<i>Key Terms</i>	159	•	<i>Review Questions</i>	159
• <i>Vital Organizational Management Issues</i>	160	•	<i>Vital Organizational Technology Issues</i>	160	•	<i>Projects and Exercises</i>	160
• <i>Lab Exercise 5-1 Firewalls</i>	161	•	<i>Case 5-1 Prevention, Defense, and Protection</i>	161	•	<i>Case 5-2 Google Hacking</i>	161
• <i>Appendix 5-1 Prototype Security Training Outline</i>	161						

Chapter 6 Managing System Protection 166

Introduction 166

Internal Threats: The Users 166

Helping the User: Safe Web Surfing 170

Divide and Conquer 171

Securing Computer Systems 173

Securing Workstations 173

Limit Shares on Your Computer 174

Dangers of ActiveX, Java, and JavaScript 175

Securing Servers 176

Securing Networks 178

Penetration Testing 179

Testing Physical Security 180

Protecting (Hardening) a System: The 6 P's 180

Patch 181

Ports 181

Protect 182

Policies 182

Probe 182

Physical 183

<i>Chapter Summary</i>	183	•	<i>Key Terms</i>	183	•	<i>Review Questions</i>	184
• <i>Vital Organizational Management Issues</i>	184	•	<i>Vital Organizational Technology Issues</i>	185	•	<i>Projects and Exercises</i>	185
• <i>Lab Exercise 6-1 Cracking Passwords</i>	186	•	<i>Case 6-1 Creating Management Policy</i>	186	•	<i>Appendix 6-1 10 Top Ways to Protect from Web Threats</i>	186
• <i>Appendix 6-2 Applying the OSI Seven Layer Network Model to Information Security</i>	189						

Chapter 7 Cryptography and Its Applications 191

Introduction 191

Introduction to Cryptography 191

Cryptography 192

Encryption 192

Types of Cryptography 193

Hash Functions 196

Securing Passwords 197

Digital Signatures 197

Securing EDI 197

Use of Asymmetric and Symmetric Cryptography 197

Public Key Infrastructure 198

Certificate Authority 198

Registration Authority 199

Certificate Repository 199

Use of a Digital Certificate and Certificate Authority 199

Secure Socket Layer 201

Virtual Private Networks 203

Secure Email 203

Management Concerns 204

SSL VPNs 204

Security Protocol 205

Chapter Summary 205 • Key Terms 206 • Review Questions 206
• Vital Organizational Management Issues 207 • Vital Organizational Technology Issues 207 • Projects and Exercises 207 • Lab Exercise 7-1 Cracking Passwords 208 • Lab Exercise 7-2 Testing Encryption 208 • Case 7-1 Protecting the Data 208 • Case 7-2 Protecting the Data 208

Chapter 8 Wireless Security 210

Introduction 210

Threats to Wireless 210

Microwave, MMDS/LMDS, WiMax, WiFi, and Satellite 211

Cellular Telephone 211

Bluetooth 212

Radio Frequency Identification 212

Packet Radio (IEEE 802.11) 213

Wireless Issues 213

Number of Access Points 213

Software Differences from Back Office 214

Bandwidth, Interoperability, Roaming, and Power Levels 215

Critical Equipment 215

Interference and Health Concerns 216

E-911 and VoIP 216

Major Threats to IEEE 802.11 (WiFi) Networks 217

Rogue Access Point 217

Malicious Association 217

Man-in-the-Middle 217

MAC Address Spoofing 218

Denial-of-Service Attacks 218

Major Issues with WiFi Wireless Access Points 218

WiFi Spread Spectrum 219

Safe Wireless Practices 219

Number 7: Change Default Service Set Identifier 221

Number 16: Assign Static IP Addresses to
Devices (no DHCP) 222

Number 14: Enable MAC Address Filtering 222

Number 10: Disable SSID Broadcast 224

Number 1: Change Default Administrator
Passwords (and Usernames) 225

Number 15: Change Default IP Subnet That
Wireless Router Is Preset to (192.168.1.0) 226

Enable Encryption: Number 3—WPA;
Number 6—WEP 227

Number 11: Keep Wireless Hardware's
Firmware Updated 227

Number 2: Place a Firewall Between the LAN
and All Access Points 227

Number 9: Position the Router or Access Point
Safely 227

Number 4: Set a Wireless Policy 228

Number 17: Turn Off the Network During
Extended Periods of Non-use 228

Number 13: Do Not Auto-Connect to
Open WiFi Networks 228

Number 5: Require VPN Connection for
Off-Site Users 229

Number 8: Do Not Allow the MAC Address to
Be Broadcast 229

Number 12: Limit Shares on Your Computer 229

Other Features 229

Buy Better Equipment 229

Conclusions 229

Chapter Summary 231 • Key Terms 231 • Review Questions 231
• Vital Organizational Management Issues 232 • Vital Organizational Technology Issues 232 • Projects and Exercises 232 • Lab Exercise 8-1 Access Point Intrusion 233 • Case 8-1 Michael Goes Wireless 233 • Appendix 8-1 Best Practices for Wireless Network Security 233

PART III The Management and Policy Side of Security 235

Chapter 9 Disaster Planning: Preparation, Response, and Recovery 237

Introduction 237

Preparedness Starts with Risk Assessment 238

The Disaster Preparedness Plan 239

Developing the Disaster Preparedness Plan 240

Capabilities and Hazards 240

Developing the Plan 243

Control and Management 243

Communications 244

Life Safety Procedures 244

Property Protection Procedures 245

The Recovery Process 245

Administering the Recovery 245

Additional Documents 245

Review of the Plan 246

Distribute the Plan and Keep It Available 247

Practice the Plan 247

Update the Plan 247

Make Disaster Preparedness a Continuous Process 248

Information Technology and Disaster Preparedness 248

What Makes IT Different? 248

Pandemic Preparedness 250

The IT Role in Disaster Response 251

Incident Response 252

Provide the Answers Beforehand 252

Chapter Summary 252 • Key Terms 252 • Review Questions 253
• Vital Organizational Management Issues 253 • Vital Organizational Technology Issues 253 • Projects and Exercises 254 • Lab Exercise 9-1 Systems Recovery: Two Machines 254 • Lab Exercise 9-2 Systems Recovery: Datacenter 254 • Case 9-1 Michael Develops a Disaster Plan 255 • Appendix 9-1 Incident Reporting Guidelines 255

Chapter 10 Network Design and Project Management 256

Introduction 256

The Security Organization 256

Security Concerns for Information Security and Network Projects 257

The Phased Approach to Project Management 258

Phases of Telecommunications Analysis and Design 258

The Request 258

Security Risk 260

Summary of SDLC Security Concerns and Initiatives 264

Project Management in Security Projects 264

The Project Management Process as Applied
to Security Projects 265

Project Initiation 265

Solution Acquisition or Development 267

Testing and Deployment 267

Going Operational 268

Project Phase-Out 268

*Chapter Summary 269 • Key Terms 270 • Review Questions 270 •
Vital Organizational Management Issues 270 • Vital Organizational
Technology Issues 271 • Projects and Exercises 271 • Lab Exercise 10-1
Project Management 271 • Case 10-1 Michael Creates Project Team
to Review Wireless Access 272 • Appendix 10-1 A Disaster in the
Making 272*

Chapter 11 Security Management 276

Introduction 276

The Security Organization 277

Functions 277

Design 277

Organization: CIO versus CISO 278

Security Policies and Training 280

Employee Classifications and Behavior 280

Insider Threat Classes 280

Program Policies 281

Issue-Specific Policies 281

Communications Policy 282

Configuration Management Policy 282

Data Security Policy 282

Data Retention Policy 283

Encryption Policy	283
Remote Access Policy	283
Firewall and DMZ Policy	283
Incident Handling Policy	283
Wireless (and Wired) Networking Policies	284
System-Specific Policies	284
Physical Security (Surveillance and Access) Policies	284
Identity Management Policy	284
Personal Policies	285
Acceptable Use Policies	285
High Privileges Access	285
Maintenance and Monitoring	285
Incident Response	286
Incident Reporting	286
Training and Certification	287
The Security Group	288
Upper Management	288
All the Organization	289
Types of Training	289
Final Comments	290
<i>Chapter Summary 290 • Key Terms 291 • Review Questions 291</i>	
<i>• Vital Organizational Management Issues 291 • Vital Organizational Technology Issues 292 • Projects and Exercises 292 • Lab Exercise 11-1 Tabletop Exercise: Defacement 292 • Lab Exercise 11-2 Tabletop Exercise: Identity Theft 293 • Case 11-1 Appropriate Use Policies for Michael 293 • Appendix 11-1 The Challenges of a Network Manager 293 • Appendix 11-2 Sample Security Policy Manual 298</i>	

Chapter 12 Legal and Ethical Issues 314

Introduction	314
U.S. Laws Affecting Data and Network Security	314
California Security Breach Notification Act	315
Gramm–Leach–Bliley Act of 1999	317
Sarbanes–Oxley Act of 2002	318
Health Insurance Portability and Accountability Act of 1996	319
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003	320
California Anti-Phishing Act of 2005	320
Federal Information Security Management Act 2002	321

**Communications Assistance for Law Enforcement
Act of 1994 321**

Standards and Rules 322

Recommended Security Controls for Federal
Information Systems: NIST 800-53 322

FDA 21 CFR Part 11 322

E-Discovery Rules 322

SEC/NASD Retention of Business Records 323

International Laws 323

Payment Card Industry Data Security Standard 324

Avoiding User Litigation 325

Harassment and Termination inside the Perimeter 325

Acceptable Use of Organizational Resources 325

Expectations of Privacy 326

Data Collected from Web Sites 326

Ethics in Security 326

The Philosophy of Ethics 327

Ethical Hacking 328

What Ethical Hackers Do 329

Surveillance 329

Impact of Legal and Ethical Considerations 330

- Chapter Summary 330 • Key Terms 331 • Review Questions 331*
- Vital Organizational Management Issues 332 • Vital Organizational Technology Issues 332 • Projects and Exercises 332*
- Lab Exercise 12-1 Auditing Software 333 • Case 12-1 Legal Protection for Michael 334 • Case 12-2 Ethical Issues for Michael 334*
- Appendix 12-1 The Effects of Legislation on Data and Security 335*
- Appendix 12-2 Abbreviated List of Computer Crime Acts by State 342*

Acronyms List 345

Glossary 347

Index 361