Contents

Foreword xxv

Chapter 1 Facing the Cybercrime Problem Head On 1

Introduction 2

Quantifying the Crisis 3

Defining Cybercrime 4

Moving from the General to the Specific 5

Understanding the Importance of Jurisdictional Issues 6

Differentiating Crimes That Use the Net from Crimes That Depend on the Net 10

Collecting Statistical Data on Cybercrime 11

Understanding the Crime Reporting System 11

Categorizing Crimes for the National Reporting System 13

Toward a Working Definition of Cybercrime 15

U.S. Federal and State Statutes 15

International Law: The United Nations Definition of Cybercrime 17

Categorizing Cybercrime 18

Developing Categories of Cybercrimes 19

Violent or Potentially Violent Cybercrime Categories 19

Nonviolent Cybercrime Categories 23

Prioritizing Cybercrime Enforcement 33

Fighting Cybercrime 35

Determining Who Will Fight Cybercrime 35

Educating Cybercrime Fighters 37

Educating Legislators and Criminal Justice Professionals 38

Educating Information Technology Professionals 39

Educating and Engaging the Community 41

Getting Creative in the Fight Against Cybercrime 41
Using Peer Pressure to Fight Cybercrime 42
Using Technology to Fight Cybercrime 43
Finding New Ways to Protect Against Cybercrime 44
Summary 45
Frequently Asked Questions 46
Resources 47

Chapter 2 Reviewing the History of Cybercrime 49
Introduction 50
Exploring Criminality in the Days of Standalone Computers 51
Sharing More Than Time 52
The Evolution of a Word 52
Understanding Early Phreakers, Hackers, and Crackers 53
Hacking Ma Bell's Phone Network 53
Phamous Phreakers 54
Phreaking on the Other Side of the Atlantic 54
A Box for Every Color Scheme 54
From Phreaker to Hacker 55
Living on the LAN: Early Computer Network Hackers 55
How BBSs Fostered Criminal Behavior 56
How Online Services Made Cybercrime Easy 57
Introducing the ARPANet:: the Wild West of Networking 58
Sputnik Inspires ARPA 59
ARPA Turns Its Talents to Computer Technology 59
Network Applications Come into Their Own 60
The Internetwork Continues to Expand 60
The ARPANet of the 1980s 60
The Internet of the 1990s 60
The Worm Turns—and Security Becomes a Concern 61
Watching Crime Rise with the Commercialization of the Internet 61
Bringing the Cybercrime Story Up to Date 62
Understanding How New Technologies Create New Vulnerabilities 62
Why Cybercriminals Love Broadband 63
Why Cybercriminals Love Wireless 67
Why Cybercriminals Love Mobile Computing 72
Why Cybercriminals Love Sophisticated Web and E-Mail Technologies 75

Why Cybercriminals Love E-Commerce and Online Banking 80
Why Cybercriminals Love Instant Messaging 84
Why Cybercriminals Love New Operating Systems and Applications 87
Why Cybercriminals Love Standardization 87
Planning for the Future: How to Thwart Tomorrow's Cybercriminal 88
Summary 89
Frequently Asked Questions 90
Resources 91

Chapter 3 Understanding the People on the Scene 93
Introduction 94
Understanding Cybercriminals 96
Profiling Cybercriminals 98
Understanding How Profiling Works 99
Reexamining Myths and Misconceptions About Cybercriminals 102
Constructing a Profile of the Typical Cybercriminal 111
Recognizing Criminal Motivations 112
Recognizing the Limitations of Statistical Analysis 119
Categorizing Cybercriminals 119
Criminals Who Use the Net as a Tool of the Crime 120
Criminals Who Use the Net Incidentally to the Crime 127
Real-Life Noncriminals Who Commit Crimes Online 128
Understanding Cybervictims 129
Categorizing Victims of Cybercrime 130
Making the Victim Part of the Crime-Fighting Team 134
Understanding Cyberinvestigators 136
Recognizing the Characteristics of a Good Cyberinvestigator 136
Categorizing Cyberinvestigators by Skill Set 138
Recruiting and Training Cyberinvestigators 139
Facilitating Cooperation: CEOs on the Scene 140
Summary 142
Frequently Asked Questions 143
Resources 145

Chapter 4 Understanding Computer Basics 147
Introduction 148
Understanding Computer Hardware 149
Looking Inside the Machine 150
Components of a Digital Computer 150
The Role of the Motherboard 151
The Roles of the Processor and Memory 153
The Role of Storage Media 157
Why This Matters to the Investigator 163
The Language of the Machine 164
Wandering Through a World of Numbers 165
Who's on Which Base? 165
Understanding the Binary Numbering System 166
Converting Between Binary and Decimal 167
Converting Between Binary and Hexadecimal 167
Converting Text to Binary 168
Encoding Nontext Files 169
Why This Matters to the Investigator 169
Understanding Computer Operating Systems 171
Understanding the Role of the Operating System Software 172
Differentiating Between Multitasking and Multiprocessing Types 173
Multitasking 173
Multiprocessing 174
Differentiating Between Proprietary and Open Source Operating Systems 175
An Overview of Commonly Used Operating Systems 177
Understanding DOS 177
Windows 1.*x* Through 3.*x* 179
Windows 9*x* (95, 95b, 95c, 98, 98SE, and ME) 181
Windows NT 183
Windows 2000 185
Windows XP 186
Linux/UNIX 188
Other Operating Systems 190
Understanding File Systems 193
FAT12 193
FAT16 194

VFAT 194
FAT32 194
NTFS 195
Other File Systems 196
Summary 197
Frequently Asked Questions 198
Resources 199

Chapter 5 Understanding Networking Basics 201
Introduction 202
Understanding How Computers Communicate on a Network 203
Sending Bits and Bytes Across a Network 204
Digital and Analog Signaling Methods 205
How Multiplexing Works 207
Directional Factors 208
Timing Factors 209
Signal Interference 210
Packets, Segments, Datagrams, and Frames 211
Access Control Methods 212
Network Types and Topologies 213
Why This Matters to the Investigator 215
Understanding Networking Models and Standards 215
The OSI Networking Model 216
The DoD Networking Model 218
The Physical/Data Link Layer Standards 220
Why This Matters to the Investigator 220
Understanding Network Hardware 221
The Role of the NIC 221
The Role of the Network Media 221
The Roles of Network Connectivity Devices 223
Why This Matters to the Investigator 231
Understanding Network Software 231
Understanding Client/Server Computing 232
Server Software 235
Client Software 236
Network File Systems and File Sharing Protocols 237
A Matter of (Networking) Protocol 238
Understanding the TCP/IP Protocols Used on the Internet 240

The Need for Standardized Protocols 240
A Brief History of TCP/IP 241
The Internet Protocol and IP Addressing 242
How Routing Works 249
The Transport Layer Protocols 254
The MAC Address 257
Name Resolution 257
TCP/IP Utilities 263
Network Monitoring Tools 269
Why This Matters to the Investigator 272
Summary 273
Frequently Asked Questions 274
Resources 277
Chapter 6 Understanding Network Intrusions and Attacks 279
Introduction 280
Understanding Network Intrusions and Attacks 282
Intrusions vs. Attacks 283
Recognizing Direct vs. Distributed Attacks 284
Automated Attacks 286
Accidental "Attacks" 287
Preventing Intentional Internal Security Breaches 288
Preventing Unauthorized External Intrusions 289
Planning for Firewall Failures 290
External Intruders with Internal Access 290
Recognizing the "Fact of the Attack" 291
Identifying and Categorizing Attack Types 292
Recognizing Pre-intrusion/Attack Activities 292
Port Scans 294
Address Spoofing 297
IP Spoofing 298
ARP Spoofing 298
DNS Spoofing 299
Placement of Trojans 300
Placement of Tracking Devices and Software 300
Placement of Packet Capture and Protocol Analyzer Software 302
Prevention and Response 304
Understanding Password Cracking 305

Brute Force 306
Exploitation of Stored Passwords 309
Interception of Passwords 311
Password Decryption Software 312
Social Engineering 313
Prevention and Response 314
General Password Protection Measures 314
Protecting the Network Against Social Engineers 315
Understanding Technical Exploits 315
Protocol Exploits 316
DoS Attacks That Exploit TCP/IP 316
Source Routing Attacks 323
Other Protocol Exploits 324
Application Exploits 324
Bug Exploits 324
Mail Bombs 325
Browser Exploits 325
Web Server Exploits 327
Buffer Overflows 328
Operating System Exploits 329
The WinNuke Out-of-Band Attack 329
Windows Registry Attacks 329
Other Windows Exploits 330
UNIX Exploits 331
Router Exploits 332
Prevention and Response 333
Attacking with Trojans,Viruses, and Worms 334
Trojans 336
Viruses 337
Worms 338
Prevention and Response 339
Hacking for Nontechies 340
The Script Kiddie Phenomenon 340
The "Point and Click" Hacker 341
Prevention and Response 342
Summary 343
Frequently Asked Questions 344
Resources 346

Chapter 7 Understanding Cybercrime Prevention 349

Introduction 350

Understanding Network Security Concepts 351

Applying Security Planning Basics 352

Defining Security 352

The Importance of Multilayered Security 353

The Intrusion Triangle 353

Removing Intrusion Opportunities 354

Talking the Talk: Security Terminology 355

Importance of Physical Security 357

Protecting the Servers 359

Keeping Workstations Secure 359

Protecting Network Devices 360

Understanding Basic Cryptography Concepts 364

Understanding the Purposes of Cryptographic Security 364

Authenticating Identity 366

Providing Confidentiality of Data 372

Ensuring Data Integrity 372

Basic Cryptography Concepts 373

Scrambling Text with Codes and Ciphers 373

What Is Encryption? 376

Securing Data with Cryptographic Algorithms 378

How Encryption Is Used in Information Security 380

What Is Steganography? 384

Modern Decryption Methods 385

Cybercriminals' Use of Encryption and Steganography 386

Making the Most of Hardware and Software Security 387

Implementing Hardware-Based Security 387

Hardware-Based Firewalls 387

Authentication Devices 388

Implementing Software-Based Security 391

Cryptographic Software 391

Digital Certificates 392

The Public Key Infrastructure 392

Software-Based Firewalls 393

Understanding Firewalls 394

How Firewalls Use Layered Filtering 395

Packet Filtering 395
Circuit Filtering 396
Application Filtering 397
Integrated Intrusion Detection 398
Forming an Incident Response Team 398
Designing and Implementing Security Policies 401
Understanding Policy-Based Security 401
What Is a Security Policy? 402
Why This Matters to the Investigator 403
Evaluating Security Needs 404
Components of an Organizational Security Plan 404
Defining Areas of Responsibility 404
Analyzing Risk Factors 406
Assessing Threats and Threat Levels 407
Analyzing Organizational and Network Vulnerabilities 409
Analyzing Organizational Factors 412
Considering Legal Factors 413
Analyzing Cost Factors 413
Assessing Security Solutions 414
Complying with Security Standards 415
Government Security Ratings 415
Utilizing Model Policies 416
Defining Policy Areas 417
Password Policies 417
Other Common Policy Areas 420
Developing the Policy Document 421
Establishing Scope and Priorities 422
Policy Development Guidelines 422
Policy Document Organization 423
Educating Network Users on Security Issues 425
Policy Enforcement 425
Policy Dissemination 426
Ongoing Assessment and Policy Update 426
Summary 427
Frequently Asked Questions 428
Resources 430

Chapter 8 Implementing System Security 431
Introduction 432
How Can Systems Be Secured? 433
The Security Mentality 433
Elements of System Security 435
Implementing Broadband Security Measures 436
Broadband Security Issues 439
Deploying Antivirus Software 441
Defining Strong User Passwords 444
Setting Access Permissions 444
Disabling File and Print Sharing 445
Using NAT 446
Deploying a Firewall 448
Disabling Unneeded Services 449
Configuring System Auditing 449
Implementing Browser and E-Mail Security 452
Types of Dangerous Code 454
JavaScript 454
ActiveX 455
Java 455
Making Browsers and E-Mail Clients More Secure 456
Restricting Programming Languages 456
Keep Security Patches Current 457
Cookie Awareness 457
Securing Web Browser Software 458
Securing Microsoft Internet Explorer 458
Securing Netscape Navigator 462
Securing Opera 464
Implementing Web Server Security 465
DMZ vs. Stronghold 466
Isolating the Web Server 467
Web Server Lockdown 468
Managing Access Control 468
Handling Directory and Data Structures 468
Scripting Vulnerabilities 469
Logging Activity 470
Backups 470

Maintaining Integrity 470
Rogue Web Servers 471
Understanding Security and Microsoft Operating Systems 471
General Microsoft Security Issues 472
NetBIOS 472
Widespread Automated Functionality 473
IRDP Vulnerability 474
NIC Bindings 474
Securing Windows 9*x* Computers 475
Securing a Windows NT 4.0 Network 478
Securing a Windows 2000 Network 481
Windows .NET: The Future of Windows Security 483
Understanding Security and UNIX/Linux Operating Systems 483
Understanding Security and Macintosh Operating Systems 487
Understanding Mainframe Security 489
Understanding Wireless Security 490
Summary 493
Frequently Asked Questions 494
Resources 495

Chapter 9 Implementing Cybercrime Detection Techniques 499
Introduction 500
Security Auditing and Log Files 502
Auditing for Windows Platforms 503
Auditing for UNIX and Linux Platforms 508
Firewall Logs, Reports, Alarms, and Alerts 510
Understanding E-Mail Headers 516
Tracing a Domain Name or IP Address 522
Commercial Intrusion Detection Systems 524
Characterizing Intrusion Detection Systems 525
Commercial IDS Players 530
IP Spoofing and Other Antidetection Tactics 532
Honeypots, Honeynets, and Other “Cyberstings” 533
Summary 536
Frequently Asked Questions 539
Resources 542

Chapter 10 Collecting and Preserving Digital Evidence 545
Introduction 546
Understanding the Role of Evidence in a Criminal Case 548
Defining Evidence 549
Admissibility of Evidence 551
Forensic Examination Standards 552
Collecting Digital Evidence 552
The Role of First Responders 553
The Role of Investigators 554
The Role of Crime Scene Technicians 555
Preserving Digital Evidence 558
Preserving Volatile Data 559
Disk Imaging 560
A History of Disk Imaging 560
Imaging Software 561
Standalone Imaging Tools 563
Role of Imaging in Computer Forensics 563
"Snapshot" Tools and File Copying 563
Special Considerations 564
Environmental Factors 564
Retaining Time and Datestamps 565
Preserving Data on PDAs and Handheld Computers 565
Recovering Digital Evidence 566
Recovering "Deleted" and "Erased" Data 567
Decrypting Encrypted Data 568
Finding Hidden Data 568
Where Data Hides 569
Detecting Steganographic Data 569
Alternate Datastreams 570
Methods for Hiding Files 571
The Recycle Bin 572
Locating Forgotten Evidence 572
Web Caches and URL Histories 572
Temp Files 574
Swap and Page Files 575
Recovering Data from Backups 577

Defeating Data Recovery Techniques 578
Overwriting the Disk 579
Degaussing or Demagnetizing 580
Physically Destroying the Disk 580
Documenting Evidence 581
Evidence Tagging and Marking 581
Evidence Logs 581
Documenting Evidence Analysis 582
Documenting the Chain of Custody 583
Computer Forensics Resources 583
Computer Forensics Training and Certification 584
Computer Forensics Equipment and Software 585
Computer Forensics Services 586
Computer Forensics Information 587
Understanding Legal Issues 587
Searching and Seizing Digital Evidence 588
U.S. Constitutional Issues 589
Search Warrant Requirements 591
Search Without Warrant 594
Seizure of Digital Evidence 597
Forfeiture Laws 598
Privacy Laws 598
The Effects of the U.S. Patriot Act 599
Summary 602
Frequently Asked Questions 603
Resources 605

Chapter 11 Building the Cybercrime Case 607

Introduction 608
Major Factors Complicating Prosecution 609
Difficulty of Defining the Crime 609
Bodies of Law 610
Types of Law 616
Levels of Law 618
Basic Criminal Justice Theory 620
Elements of the Offense 624
Level and Burden of Proof 625

Jurisdictional Issues 626
Defining Jurisdiction 626
Statutory Law Pertaining to Jurisdiction 629
Case Law Pertaining to Jurisdiction 630
International Complications 631
Practical Considerations 631
The Nature of the Evidence 632
Human Factors 633
Law Enforcement "Attitude" 633
The High-Tech Lifestyle 635
Natural-Born Adversaries? 635
Overcoming Obstacles to Effective Prosecution 636
The Investigative Process 637
Investigative Tools 639
Steps in an Investigation 646
Defining Areas of Responsibility 650
Testifying in a Cybercrime Case 650
The Trial Process 651
Testifying as an Evidentiary Witness 652
Testifying as an Expert Witness 652
Giving Direct Testimony 653
Cross-Examination Tactics 654
Using Notes and Visual Aids 654
Summary 656
Frequently Asked Questions 657
Resources 658

Afterword 659

Appendix 663

Index 699