Contents

Part I Introducing Cybercrimes

1 A Pragmatic, Experiential Definition of Computer Crimes 3
1.1 Introducing Computer Crimes 3
1.1.1 The Melissa Virus: The Turning Point 3
1.1.2 Cybercrimes in Early 2001 8
1.1.3 Defining Technical Cybercrime 9
1.2 The Battle to Control the Computing Process 11
1.2.1 The Nature of the Battle 11
1.2.2 The Cyberbattlefield 11
1.3 Tools for Fighting the Battle to Control the Computing Process 18
1.3.1 Defining Tools 18
1.3.2 The Attacker's Technical Tools 18
1.3.3 The Attacker's Social Tools 20
1.3.4 The Defender's Tools 21
1.4 The Convenience Overshoot Warning 22
References 23

Part II Computing and Networking Technology and Cybercrimes

2 Unauthorized Intrusions and Denial of Service 27
2.1 Unauthorized Intrusions 27
2.1.1 Tools to Exploit Unauthorized Intrusions 28
2.1.2 Deployment of Toolkits for Unauthorized Intrusions 34
2.2 Denial of Service 40
2.2.1 Different Manifestations of DDoS Attacks 41
2.2.2 Toolkits for DDoS 43
References 44

3 Malicious Code 45
3.1 Introduction 45
3.1.1 Trends that Facilitate Malicious Code to Thrive 47

Bibliografische Informationen
http://d-nb.info/1002540666

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

3.2 The Nature of Malicious Code ... 48
3.2.1 Operational Phases of Malicious Code ... 50
3.3 Categories of Malicious Code ... 51
3.3.1 Viruses ... 51
3.3.2 Worms ... 52
3.3.3 Trojan Horse Programs ... 56
3.3.4 Zombies ... 56
3.3.5 Adware ... 57
3.3.6 Malicious Mobile Code ... 58
3.4 A Closer Look into the Inner Workings of Malicious Code ... 58
3.4.1 Code Red ... 58
3.4.2 Nimda ... 60
3.4.3 Slammer ... 61
3.5 Malicious Code Creation Process ... 62
3.6 Techniques to Defeat Malicious Code ... 64
3.6.1 Host-Based Protection ... 64
3.6.2 Network-Based Protection ... 66
3.7 Vulnerability Management and Patching ... 67
3.8 The Future of Malicious Code and New Mitigation Approaches ... 68
3.8.1 The Future of Malicious Code ... 68
3.8.2 The Future of Mitigation Approaches ... 69
References ... 71

4 Restricting Anti-Circumvention Devices ... 73
4.1 Background: The Difference Between Digital and Analog ... 73
4.2 Law is Inadequate and Technology is Necessitated ... 75
4.3 Content Protection Efforts ... 76
4.3.1 Copy Prevention ... 76
4.3.2 Licenses and Legal Agreements ... 77
4.3.3 Data Format as Barriers ... 77
4.3.4 Software-Based Copy-Protection Systems ... 78
4.3.5 Digital Millennium Copyright Act ... 79
4.3.6 Conditional Access ... 79
4.4 The Nature of the Threat ... 80
4.4.1 Casual Copiers ... 80
4.4.2 Peer-to-Peer Pirates ... 80
4.4.3 Professional Pirates Who Profit from Distributing Large Volumes ... 81
4.5 What Can and Cannot be Protected? ... 81
4.5.1 The Price Point ... 82
4.5.2 Cheaper to Buy than to Steal ... 82
4.6 Logical Consequences ... 83
4.6.1 Closed Architecture ... 83
4.6.2 Open Architecture ... 84

4.7 A Primer on Encryption 84
4.7.1 Nomenclature 85
4.7.2 Ciphers, Keys, and Security 85
4.7.3 Secret-Key Encryption 86
4.7.4 Public-Key Encryption 87
4.8 Content-Protection Approaches 87
4.8.1 Systems Providing Read Access to Content 88
4.8.2 System-Level Content Protection 91
4.8.3 Microsoft's and Intel's Directions 92
4.9 Summary and Conclusions 93
References 93

5 Information Security 95
5.1 Introduction 95
5.2 Current Technological Threats 96
5.2.1 Trusted Computing 96
5.2.2 Software Weaknesses: A Root Cause 98
5.2.3 Malicious Code: Viruses and Worms 99
5.2.4 Mobile Code 101
5.2.5 Illicit Connections 103
5.2.6 Eavesdropping 105
5.2.7 Network-Based Attacks 108
5.2.8 Denial of Service (DoS) 109
5.2.9 Patchwork Quilt 110
5.3 Technical Approaches to Solving Security Problems 110
5.3.1 Antivirus Software 111
5.3.2 Demobilizing Code 112
5.3.3 Encryption 114
5.3.4 Firewalls 115
5.3.5 Intrusion Detection Systems 117
5.3.6 Virtual Private Networks (VPNs) 118
5.3.7 Physical Security Measures 118
5.4 People Problems 119
5.4.1 Failure to Report Security Problems 121
5.4.2 Policy 123
5.5 Summary 124
References 124

Part III Economic Impact of Cybercrimes

6 Economic Consequences 129
6.1 Introduction 129
6.2 Societal Benefits of Measuring Economic Impact of Cybercrimes 130
6.2.1 Allocation of Funding and Expenses 131

6.3 Malicious Code Attacks 132
6.3.1 Proposed Methodology to Measure Economic Impact 133
6.3.2 Data Acquisition and Computing Economic Impact 136
6.3.3 Incident Report to Facilitate Data Acquisition 138
References 140

7 **Infosecurity Funding** 141
7.1 The INFOSEC Research Council 142
7.2 The Current State of Infosec Research 145
7.2.1 Data Collection 145
7.2.2 Projects and the List of "Hard Problems" 145
7.2.3 How Much Money is Being Spend and Where? 146
7.3 Research Goals 146
7.3.1 Recommendations 147
References 150

8 **Information and Computer Security Risk Management** 151
8.1 Private Industry Effectiveness: The Need for a Risk Management Perspective 151
8.2 Definitions of Risk and Enterprise Risk 152
8.3 Risk Management and the Risk Management Process 152
8.4 Risk Management Analysis 153
8.5 Risk Prevention 157
8.6 Risk Mitigation 159
8.7 The Need for a Security Breach Incident Response Plan 160
8.8 Risk Financing 160
8.9 Summary 162
References 163

9 **Trend Analysis for Digital Risk Management** 165
References 170

Part IV Critical Infrastructure Protection and Cybercrimes

10 **Evolutionary History of Critical Infrastructure Protection in the USA** 173
10.1 What is "Critical Infrastructure"? 174
10.2 US CIP Policy 176
10.2.1 The Threat 176
10.2.2 The Structure and Evolution of US CIP Efforts 180
10.3 Criminal and Intelligence Authorities and CIP 184
10.3.1 CIP and National Security 184
10.3.2 Identifying whether a Cyberattack Poses a National Security Concern 185

10.3.3 The Criminal Law Enforcement and National Intelligence Divide 186
10.3.4 U.S. Military CIP and Cyber Activities 190
10.3.5 Changes in Federal Law in Support of CIP 194
References 195

11 Critical Infrastructure Protection Policy in the US 199

12 Scientific and Technological Nature of Critical Infrastructure Vulnerabilities 203
12.1 The Electric Power Grid 203
12.2 Other Critical Infrastructures 207
References 208

13 Internet Infrastructure Attacks 209
13.1 Internet Router Attacks 209
13.2 Domain Name Services (DNS) Attacks 211

Part V Psycho-Social Impact of Cybercrimes

14 The Psyche of Cybercriminals: A Psycho-Social Perspective 217
14.1 Introduction 217
14.2 Who is Drawn to Cybercrimes 217
14.2.1 Taxonomy 218
14.2.2 Limitations 222
14.3 Why are Cybercriminals Attracted to Commit Crimes 223
14.3.1 Social Learning Theory 223
14.3.2 Moral Disengagement 226
14.3.3 Anonymity 228
14.4 Strategies to Contain Cybercriminal Behaviors: Deterrence and Rehabilitation 229
14.4.1 Cybercrime Laws 229
14.4.2 Social Sanctions 231
14.4.3 Education 233
14.5 Conclusions 234
References 235

Part VI Cybercrime Regulation Through Civil and Criminal Penalties

15 Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US 239
15.1 Introduction 239
15.2 Indirect Regulation Through Law 242
15.2.1 Intellectual Property Law 242
15.2.2 Financial and Medical Privacy Law 243

15.2.3 Identity Theft Law ... 247
15.2.4 Indirect Regulation Through Laws Imposing Liability and Through the Establishment of Best Practices and Standards ... 249
15.2.5 Best Practices ... 250
15.2.6 Federal Cybersecurity Standards ... 250
15.3 Indirect Regulation Through Market Forces ... 252
15.3.1 Cyberinsurance Markets ... 252
15.3.2 Public–Private Information Sharing Initiatives ... 254
15.3.3 Federally-Funded Research and Development ... 259
15.3.4 Federally-Funded Educational Programs ... 261
15.4 Indirect Regulation Through Social Norms ... 262
15.4.1 Cybercitizen Partnership ... 262
15.5 Conclusions ... 262
References ... 263

16 Criminal Regulations ... 265
16.1 Substantive Laws Addressing Digital Crimes ... 265
16.1.1 Computer and Network Crimes ... 265
16.1.2 Intellectual Property Violations ... 277
16.1.3 Crimes Against Persons & Other Unlawful Digital Conduct ... 282
16.1.4 Wiretap Act ... 285
16.2 Challenges Created by Computer and Network Crimes ... 286
16.2.1 Jurisdiction ... 286
16.2.2 Masking Techniques ... 289
16.2.3 Reporting ... 290
16.3 Procedural Laws Addressing Computer and Network Crimes ... 292
16.3.1 Computer and Network Crimes ... 292
16.3.2 Real Time Transmission and Interception ... 296
16.3.3 Stored Electronic Communications ... 299
16.4 Investigatory Challenges ... 302
16.4.1 Jurisdiction ... 302
16.4.2 Venue ... 303
16.5 Operational Challenges ... 304
16.6 Technological Challenges ... 305
16.6.1 Diverse Business Environments ... 305
16.6.2 Wireless ... 306
16.6.3 Satellite-Based Telephony ... 306
References ... 307

Part VII International Character of Cybercrimes

17 International Dimensions of Cybercrime 311
17.1 A Global Perspective on Cybercrime....................................311
17.2 The Globalization of Crime....................................312
17.3 A New Way to View Crime in the Global Village 315
17.4 The Networked World....................................317
17.5 The Love Bug and International Cybercrime: A Case Study 317
17.6 International Law and Cybercrime 320
17.6.1 Jurisdiction....................................321
17.6.2 Extradition and Potential Conflict of Nations' Laws 323
17.6.3 Search and Seizure 323
17.7 International Efforts to Combat Cybercrime....................................325
17.7.1 The Organization for Economic Cooperation and Development (OECD) 326
17.7.2 The United Nations....................................327
17.7.3 The Group of 8 (G-8)....................................328
17.7.4 The Council of Europe 330
17.7.5 Other Fora and Interpol 331
17.8 The Importance of Building International Consensus on Cybercrimes....................................333
17.9 Conclusion....................................334
References....................................336

18 Formidable Challenges Posed by Cybercrimes....................................341
18.1 Electronic Medical Records and Cybercrimes....................................342
18.1.1 Vulnerability of EMRs 343
18.1.2 Consequences of EMRs Compromises....................................344
18.1.3 Far-Reaching Benefits of EMRs?....................................345
18.1.4 A Formidable Challenge to EMRs and EMBs? 347
18.2 EM-Money and Cybercrimes....................................348
18.2.1 The Origin of Money 348
18.2.2 The Evolution of Money 348
18.2.3 Characteristics of Future Money....................................349
18.2.4 EM-Money: A New Manifestation of Money 350
18.2.5 Formidable Challenges to EM-Money....................................352
18.3 Student Academic Records, Online Education, and Cybercrimes....................................353
18.3.1 Relocating Universities into Cyberspace 354
18.3.2 The Vulnerabilities of Education and Learning in Cyberspace 355
18.3.3 Summary 358
18.4 The Concept of Witnesses and Cybercrimes....................................359
18.5 The Scope and Gravity of Cybercrimes....................................360
References....................................361

Part VIII Mitigation of Cybercrimes

19 Increasing Attack Costs & Risks and Reducing Attack Motivations...365
19.1 Behavioral Science Research and Traditional Deterrence............366
19.1.1 The Criminal Justice System, by itself, does not Adequately Prevent Crime...............................366
19.1.2 Why Does Anyone Obey the Law: Social Stigma and Conscience? 367
19.1.3 Need for a Holistic Crime Prevention Approach............368
19.1.4 Need to Target Cost, Risk, and Motivation..................368
19.1.5 Summary...369
19.2 Impact of Traditional Deterrence on Cybercrimes....................369
19.2.1 Research into Traditional Deterrence........................369
19.2.2 Low Apprehension Probability for Cybercrimes..370
19.2.3 Minimal Social Stigma from Computing Crimes 370
19.2.4 Abundance of Vulnerable Targets............................370
19.2.5 Summary...374
19.3 Relative Effectiveness of Raising Attack Costs and Attack Risks and Reducing Attack Motivation 374
References...375

Part IX Future of Cybercrimes: Who Will Have the Last Word?

20 Nature of Cyberattacks in the Future......................................379
20.1 The Engineering Fundamentals of Networked Systems..............380
20.2 Potential Advances in Networked System Stemming from its Fundamental Nature 381
20.3 Long-Term Innovations in Networked Systems 388
20.3.1 Generalized Networks..388
20.3.2 Strictly Inanimate Networked Systems......................389
20.3.3 Highly Interlinked Networked Systems 390
20.3.4 Quantum Entanglement Technology for Packet Transport?.......................................393
20.3.5 Fundamental Insight into the Nature of Security 394
20.4 New Approaches to Secure Networked System Design for the Future 395
20.5 Who Will Have the Last Word in Cybercrimes?.......................397
References...398

Introducing the Authors...401

Index...411