

Fighting Computer Crime

A NEW FRAMEWORK FOR
PROTECTING INFORMATION

DONN B. PARKER

WILEY COMPUTER PUBLISHING



John Wiley & Sons, Inc.

New York • Chichester • Weinheim • Brisbane • Singapore • Toronto

CONTENTS

Foreword	vii	
Preface	xiii	
<i>Chapter 1 The Myth of Information Security</i>		<i>1</i>
The Big Picture	2	
Learning from Experience	3	
Weaknesses in Information Security Controls	5	
The Human Factor	6	
How We Got into This Mess	7	
The Extent of Crime in Cyberspace	10	
The Cyberspace Crimoid Syndrome	11	
Back to Basics	14	
Fortifying Installed Controls	19	
How Do We Fix Information Security?	23	
<i>Chapter 2 What Are We Protecting?</i>		<i>27</i>
Primary Characteristics of Information	28	
Kinds of Information	31	
Representations of Information	41	
Forms of Information	42	
Media	44	

Contents

Owners of Information	50	
Conclusions	55	
Chapters	<i>The Rise of Cybercrime</i>	57
Abuse and Misuse	58	
Trends of Business Crime	62	
The Role of Collusion in Business Crime	66	
Small-Business Crime in Cyberspace	67	
The Rise of Cybercrimoids	69	
Reporting Cybercrimes	70	
Distorted Portrayals of Cybercrime in the Entertainment World	74	
Cybercrime Law	77	
The Future of Cybercrime	79	
Chapter 4	<i>Computer Abuse and Misuse</i>	81
Computer Viruses and Related Crimes	82	
Data Diddling	94	
Superzapping	94	
Computer Larceny	95	
Extortion and Sabotage	96	
Information Anarchy Using Encryption	96	
Desktop Forgery and Counterfeiting	98	
Software Piracy	99	
Perceived Loss of Privacy in Cyberspace	102	
International Commercial Espionage	105	
Information Warfare	109	
Summary of Computer Abuse and Misuse	110	
Chapter 5	<i>Network Abuse and Misuse</i>	113
Internet Crime	114	
LANarchy	125	
Electronic Banking and Electronic Data Interchange (EDI) Fraud	125	
Automated Crime	129	
Conclusions	132	
Chapter 6	<i>Cyberspace Abusers and Misusers</i>	135
Characterizing the Perpetrators of Cybercrime	136	
Motives and the Cybercriminal	133	
Seven Kinds of Cybercriminals	144	
The Cybercrime Rationalization	146	
Social Engineering and Gullibility	148	
A Summary of Protective Techniques	155	
Chapter 7	<i>The Disastrous Hacker Culture</i>	157
What Is Hacking?	158	
Who Is a Hacker?	162	
How Much Hacking Is There?	164	
How a Hacker Hacks	165	
Understanding the Hacker Culture	168	

Hacking As a Crime	174	
Conferences Where Hackers Gather Together	177	
The New Generation of Hackers	179	
How to Treat Our Hacker Adversaries	184	
Chapter 8 The Artisans of Information Security		189
Occupational Organization	190	
The Role of Criminal Justice in Information Security	196	
A Multidisciplinary Approach to Information Security	197	
Advancing the Strategic Values of Information Security in Business	203	
Chapter 9 The Current Foundation for Information Security		211
The Current Framework Model	212	
Generally Accepted System Security Principles	214	
The British Code of Practice	217	
CobiT: Control Objectives for Information and Related Technology Framework	220	
Conflicting Definitions: Message Confidentiality, Integrity, and Authenticity	221	
Neumann's View of Information Security Terms	224	
Implications of the Confusion Surrounding Security Terminology	227	
Conclusion	228	
Chapter 10 A New Framework for Information Security		229
Proposal for a New Information Security Framework	230	
Six Essential Foundation Elements	230	
Comprehensive List of Information Losses	240	
The Functions of Information Security	252	
Threats, Assets, Vulnerabilities Model	255	
Clark-Wilson Integrity Model: A Framework for Business Applications Security	256	
Conclusions	260	
Chapter 11 Information Security Assessments		261
Risk Assessment	262	
Problems with Quantitative Risk Assessment Methodologies	269	
Alternative Techniques	279	
The Baseline Approach	282	
Chapter 12 How to Conduct a Baseline Security Assessment		295
Good Security in a Small Business or Home Environment	295	
A Summary of the Baseline Security Review Process	297	
Guidelines for Conducting Baseline Information Security Reviews	301	
A Methodology for Information Owners Untrained in Information Security	301	
The Methodology for Information Security Experts	303	

Chapter 13	<i>Good and Bad Control Objectives</i>	325
	Control Effectiveness Strategy	327
	Use of Elements to Identify and Select Control Objectives	330
	How to Use the Guides to the Control Principles	332
	Descriptions of the Guides	334
	Conclusion	358
Chapter 14	<i>Tactics for Effective Information Security</i>	361
	Information Security Controls for Organization Changes	362
	The Changing Needs for Confidentiality and Classification	369
	Cryptography	372
	Authenticated Logon Control	382
	Testing System Security	393
	Protection from Social Engineering and Gullibility	397
	The Limitations of Technical Security	407
Chapter 15	<i>Strategies for Effective Information Security</i>	411
	Strategic Values of Information and Security	412
	Subtle Roles and Strategic Effects of Security	419
	Ethics: The Essence of Good Security	421
	Legal Concerns	424
	Recommendations for Security Advisors and Conclusions	434
Chapter 16	<i>Organizing for Security</i>	437
	Fitting Security into the Organization	439
	The Size, Nature, and Location of Information Security Units	440
	General Methodology for Distributed Computing Security	443
	Open and Closed Distributed Environments	447
	Policies and Management Support	448
	Standards and Distributed Information Security Administrators	454
	Guidelines and Technical Support	459
	Motivating End-Users for Information Security	462
	Other Information Security Management Issues	471
Chapter 17	<i>Doing It Right and Preparing for the Next Millennium</i>	475
	Moving Information Security Forward	478
	Solving the Hacker Menace	482
	Dealing with the Privacy Problem	488
	Solving the Cryptography Information Anarchy Problem	490
	Some Final Thoughts for Better Information Security	499
	Index	501