Computer Security

COMPUTER CRIME

A Crimefighter's Handbook

David Icove, Karl Seger, & William VonStorch

O'Reilly & Associates, Inc.

Computer Crime

A Crimefighter's Handbook

David Icove, Karl Seger,
and William VonStorch

O'Reilly & Associates, Inc.
103 Morris Street, Suite A
Sebastopol, CA 95472

Table of Contents

Foreword ..... *ix*

Preface ..... *xv*
About This Book xvi
Scope of the Book xvii
Comments and Questions xix
Acknowledgments xix

Part I: Overview *1*

1: Introduction to Computer Crime *3*
Types of Attacks 5
What Laws Prohibit Computer Crime? 16
Where Are the Vulnerabilities? 17
Who Commits Computer Crimes? 22
How Can Computer Crime Be Prevented? 23
Handling Computer Crime 25

2: What Are the Crimes? *29*
Breaches of Physical Security 30
Breaches of Personnel Security 35
Breaches of Communications and Data Security 40
Breaches of Operations Security 48
Ways of Detecting Common Attacks 54

3: Who Commits Computer Crimes? *61*
Types of Offenders 61
Characteristics of Computer Criminals 65
Computer Crime Adversarial Matrix 67

4: What Are the Laws? *71*
Who Has Jurisdiction? 72
U.S. Federal Laws 73
State Laws 83
International Laws 85

Part II: Preventing Computer Crime ***87***

5: What Is at Risk? *89*
Threats, Vulnerabilities, and Countermeasures 89
Steps in Risk Analysis 92
Identifying Threats 95
Identifying Assets 96
Identifying Vulnerabilities and Countermeasures 98

6: Physical Security *103*
Basic Physical Security 104
Testing Physical Security Programs 107
Natural Disaster Checklists 110
Environmental Disaster Checklists 112
Intruder Checklists 113

7: Personnel Security *115*
Developing a Personnel Security Program 116
Types of Threats 116
Different People/Different Threats 118
Personnel Security Checklist 126

8: Communications Security *129*
Types of Networks 129
Network Communications 132
Protecting Your Network Communications 134
Communications Security Checklist 141

9: Operations Security *143*
Planning Operations Security 144
Where Do Computer Criminals Get Information? 146
Developing an Operations Security Program 150
Ongoing Operations Security 153

Part III: Handling Computer Crime ***155***

10: Planning How to Handle a Computer Crime *157*
Finding Out About a Computer Crime 158
Setting Up Detection Measures 160
Forming a Crisis Management Team 161
What to Do If the Intruder Is on the System 163
Examining Log Files and Other Evidence 168
Be Careful from the Start 171

11: Investigating a Computer Crime *175*
Calling in Law Enforcement 176
Forming an Investigative Team 176
How to Investigate 178
Preparing a Search Warrant 179
What to Bring to the Scene 181
Executing a Search Warrant 183
Getting Help from a Technical Adviser 187
Auditing Tools 188
Guidelines for Handling Evidence 189

12: Prosecuting a Computer Crime *195*
Judges and Juries 195
Evidence in Computer Crime Cases 196
Testifying in Computer Crime Cases 201
After the Prosecution 202

Part IV: Computer Crime Laws ***203***

Part V: Appendices *351*

A: Resource Summary *353*
Books 353
Periodicals 355
User Organizations 357
Emergency Response Organizations 358
Government Agencies 365
Electronic Resources 365

B: Raiding the Computer Room *369*
Warrant Requirement 370
Executing the Search Warrant 382
Conclusion 389

C: The Microcomputer as Evidence *391*
Introduction 391
Procedures for Submission and Examination of Computer Evidence 394
Conclusion 395
References 395

D: A Sample Search Warrant *397*

Glossary *411*

Index *429*

O'Reilly & Associates, Inc.

COMPUTER CRIME: A Crimefighter's Handbook

Terrorist attacks on computer centers, electronic fraud on international funds transfer networks, viruses and worms in our software, corporate espionage on business networks, and crackers breaking into systems on the Internet...Computer criminals are becoming ever more technically sophisticated, and it's an increasing challenge to keep up with their methods.

This book is for anyone who needs to know what today's computer crimes look like, how to prevent them, and how to detect, investigate, and prosecute them if they do occur. It contains basic computer security information as well as guidelines for investigators, law enforcement, and computer system managers and administrators. Also included is the text of U.S. federal, state, and international computer crime laws.

"This is more than a handbook for investigators in tracking down computer crime—it also tells you how to respond to threats and ways to avoid problems. This book shows where computing meets law enforcement."

—Cliff Stoll, author of The Cuckoo's Egg *and* Silicon Snake Oil

"This book provides an excellent primer for both the network security professional and the criminal investigator...The authors assisted in the successful conclusion of several federal investigations."

—James C. Settle, I-NET and former FBI agent

"...a very helpful and interesting book. I'm going to make sure all of the Secret Service new Electronic Crimes Special Agents get a copy to assist them."

—Bob Friel, U.S. Secret Service

"This is an excellent and worthwhile handbook for both the novice and experienced computer crime investigator. I will recommend it to my computer crime classes."

—Detective Robert M. Snyder, Columbus Ohio Police Department

"Any organization that is worried about attacks on their computer systems, especially those attached to the Internet, should run to the bookstore to pick up a copy of ***Computer Crime***. It's one-stop shopping for system administrators and law enforcers, with plenty of pointers to additional resources if needed."

—Lance J. Hoffman, Director, Institute for Computer and Telecommunications Systems Policy, School of Engineering, The George Washington University

RepKover.

Printed on Recycled Paper

ISBN 1-56592-086-4