INVESTIGATING INFORMATION-BASED CRIMES

ABOUT THE AUTHOR

An investigative writer, Ronald L. Mendell holds a Master of Science degree in Network Security from Capitol College in Laurel, Maryland. Ronald also completed additional graduate work in investigation and forensic science at National University in San Diego, California. He has the Certified Information Systems Security Professional (CISSP) designation in the information security field. Additionally, he is a Certified Legal Investigator (CLI). Currently, he serves as an Adjunct Assistant Professor of Computer Science at Austin Community College in Austin, Texas. *Investigating Information-based Crimes* is his seventh book on investigations and security. In addition to books, Ronald writes articles on information security for *The ISSA Journal* and book reviews for *Security Management.*

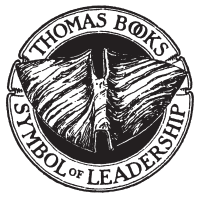
INVESTIGATING INFORMATION-BASED CRIMES

A Guide for Investigators on Crimes Against Persons Related to the Theft or Manipulation of Information Assets

By

RONALD L. MENDELL, M.S., CLI, CISSP

Adjunct Professor of Computer Science
Austin Community College
Austin, Texas
Certified Information Systems Security Professional (CISSP)
Certified Legal Investigator (CLI)



CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

ISBN 978-0-398-08871-2 (paper)
ISBN 978-0-398-08872-9 (ebook)

Library of Congress Catalog Card Number: 2012038227

With THOMAS BOOKS *careful attention is given to all details of manufacturing and design. It is the Publisher's desire to present books that are satisfactory as to their physical qualities and artistic possibilities and appropriate for their particular use.* THOMAS BOOKS *will be true to those laws of quality that assure a good name and good will.*

Printed in the United States of America
MM-R-3

Library of Congress Cataloging-in-Publication Data

Mendell, Ronald L.
Investigating information-based crimes : a guide for investigators on crimes against persons related to the theft or manipulation of information assets / by Ronald L. Mendell.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-398-08871-2 (pbk.) -- ISBN 978-0-398-08872-9 (ebook)
1. Computer crimes–Investigation. 2. Data protection. 3. Confidential communications. 4. Criminal investigation. I. Title.

HV8079.C65M464 2013
363.25′968–dc23

2012038227

PREFACE

"Take us the foxes, the little foxes that spoil the vines, for our vines have tender grapes." This imagery from the *Song of Solomon* translates into describing the information-based offenses that plague today's "vineyard of information." Information-based crimes against persons involve the theft, compromise, misuse, or manipulation of personal data or knowledge assets. These assets, which can be physical or electronic, compose every person's vulnerable dimension of facts, ideas, and knowledge particular to an individual.

Assets such as financial documents and transactions, e-mails, diaries, calendars, spreadsheets, and other personal information, such as medical records, become the target of twenty-first century "foxes." Persons victimized face the theft or exploitation of these assets by elements ranging from organized crime to freelance criminals to personal enemies. And, critical information may not be limited to data strictly within the care, custody, and control of the victim. Data available on the Web, whether in public records or on social networking sites, becomes the grist, through calculated misuse, for information-based crimes. Digitized audio and video, ever growing in our expanding surveillance culture, is another area for exploitation.

Personal information-based crimes are of two categories: those against individuals and those against an individual's assets directly. The crimes against individuals encompass disinformation (discrediting a person falsely) and misusing digitized surveillance (whether audio or video) to either commit a crime or to engage in a disinformation campaign. Crimes against information assets include identity theft (stealing PII, personally identifiable information), the theft of electronic files and/or physical records, social engineering (stealing assets through pretext), and using publicly available information online to facilitate other crimes.

Investigators will learn from the text how to evaluate the victimology in a case. How did the victim's information fall prey to attack? Why was this victim chosen? In each type of attack, the book makes suggestions for completing a vulnerability analysis on the victim's assets to determine the methods used in the suspect's attack. Once an M.O. (method of operation) be-

comes established for an UNSUB (unknown suspect), the text presents ideas on narrowing the universe of suspects and in linking them to the offense. The book also offers investigative checklists for probing into information-based crimes against persons. In addition, the narrative strives to take a psychological methodology in investigating these cases. By reading this book, private investigators and law enforcement will be armed with strategies for dealing with today's "foxes" that threaten our interconnected, global information community.

R.L.M.

ACKNOWLEDGMENTS

The author would like to thank the Austin Public Library for the use of its reference services in the preparation of this book. In addition, he thanks the University of Texas at Austin Library staff for their assistance in research for the text. Finally, special thanks go to his wife, Rebecah, for her patience and encouragement during the preparation of the manuscript.

CONTENTS

Page

Preface v

INTRODUCTION 3
Nature of Information-based Crimes 3
Crimes against People 4
Disinformation 5
Misuse of Electronic Surveillance 5
Crimes against Persons' Information Assets 6
Identity Theft 6
Via Social Engineering 7
Theft of Personal Information Repositories 7
Misuse of Online Information and Metadata Attacks 8
Thefts of Physical Information Assets 9

Chapter

1. IDENTITY THEFT 10
Main Points of Vulnerability 11
Doing a Vulnerability Analysis and Social Networking Investigations 15
Identifying Likely Suspects 18
Building Evidence Links 21
Investigative Checklist 24

2. SOCIAL ENGINEERING 26
Leakage vs. Social Penetration 32
Building a Trail to the Compromised Asset 37
Analyzing the Entry Points: Locating Information about People and Related Businesses 39

Linking Suspects to the Compromise 40
Investigative Checklist 43

3. DISINFORMATION 45
Documenting the Campaign's Extent and the Target's Infosphere 47
Social Networking 51
The Profiling of Suspects 53
Developing Linkage to Evidence 56
Investigative Checklist 57

4. DIGITAL EVIDENCE AND DIGITAL REPOSITORIES 59
Repositories in the Cloud and Information Stores 59
Storage in Digital Computers 64
Network Servers and Storage and Digital Forensics 68
Mobile Devices and Digital Forensics 70
Role of Repositories in Information-based Crime 73

5. THE THEFT OF PERSONAL INFORMATION REPOSITORIES 76
Unauthorized Copying 81
Physical Theft 82
Investigative Checklist 84

6. MISUSE OF ONLINE INFORMATION 85
Not Always Illegal Per Se 86
Publicly Available Information Provides a Foothold for Crimes 87
Developing a Victim's Information Footprint: Google Hacking, Web Application Attacks, Social Networking 91
Digital Identity Planning 96
Documenting a Suspect's Use of Publicly Available Information: Histories, Assets, Financial Data 98
Investigative Checklist 99

7. MISUSE OF ELECTRONIC SURVEILLANCE 102
Interviewing the Client or Victim 102
Tracking of Individuals and Vehicles 104

Other Methods of Tracking: Metadata on Images and in Documents, and Analyzing Online Data 108
Gaining Access Illegally to Video Surveillance 110
Illegal Interception of Digital Communications 112
Investigative Checklist 113

8. THEFT OF PHYSICAL INFORMATION ASSETS 115
Rare Books and Manuscripts 116
Documents and Personal Papers 122
Sensitive Business Documents 124
Conducting a Vulnerability Analysis 126
Identifying Suspects 128
Investigative Checklist 130

9. PSYCHOLOGICAL DIMENSIONS 133
Profiling 134
Interrogation 139
Perception Issues 141
Intelligence Gathering 145
Summary 150

10. THE FUTURE OF INFORMATION-BASED CRIMES 151
The Diary Begins 151
The Undercurrent 153
The Diary Continues 155
Thinking About Your Computer 157
Trends and Observations on the Digital Future 158

Appendix A: Checklist for Interviewing Victims 173
Appendix B: Security Checklist 176
Appendix C: Investigative Checklists 181
Glossary 195
Bibliography 199
Index 207

INVESTIGATING INFORMATION-BASED CRIMES

INTRODUCTION

Few would question that we live in an Information Age. What we know and how we store what we know securely become the fundamental issues for our times. In the not too distant past, cash or commodities like gold, silver, and other precious metals were the sole targets of thieves. As society evolved in financial sophistication, stealing and counterfeiting checks and credit cards emerged as a strong vector for crime. The, the information contained in checks, on credit cards, in bank account access codes and numbers became a valuable commodity for thieves. The current stage of evolution in criminal activity involves trafficking in stolen personally identifiable information (PII) about individuals, which includes educational, financial, medical, and vocational data. Identity theft and the stealing of financial assets are among the results of such trafficking. This book's theme is about investigating these twenty-first century information-based crimes.

NATURE OF INFORMATION-BASED CRIMES

These information-based crimes fall into two major categories: exploiting information about people and the theft or compromise of information assets. Exploiting information available online concerning individuals usually involves disinformation and/or the misuse of electronic surveillance. Crimes against individuals' information assets cover identity theft, social engineering, the theft of personal information storage areas or repositories, and the theft of physical information assets such as papers, manuscripts, or rare books. Our discussion of information-based crimes does not include scams per se, although in Chapter 9 on the "Psychological Dimensions," the text covers various inducements used by information to lure victims into surrendering personal-

ly identifiable information (PII). And, our discussion of charlatanism also receives coverage in Chapter 2 on "Social Engineering," but the focus remains on separating people from their sensitive information not just their money.

The text does not engage directly about common-law crimes such as robbery, burglary, homicide, or sexual assault. However, an important undercurrent to remember is that information theft facilitates common-law crimes in some cases. The more an attacker knows about the victim the easier a violent crime becomes to commit. However, with the exception of the theft of physical information assets, the arena or the theater of information-based crimes resides via electronic media in cyberspace. The element of physical interaction, the basis of many common-law crimes, does not enter the picture, which makes many of these crimes insidious and challenging to investigate.

CRIMES AGAINST PEOPLE

Exploiting information about people constitutes the first major division in the text's discussion. Warping or distorting the view the public has of an individual via the tools of the Internet involves disinformation. And, disinformation campaigns operate at the macro and the micro levels. The twisting of the truth about someone may originate from a widely visited website or from an online posting visited by the few. In addition to the poisonous brush strokes of disinformation, persons may also suffer from being monitored via cyberspace through unknown eyes. We live in an increasingly watchful society where our privacy and confidentiality evaporate faster than freshly applied rubbing alcohol. And electronic surveillance, like disinformation, may cling to use through malevolent actions: cyber stalking would be one, well-known example. Yet, when we go to the grocery store, use an ATM, cash a check, or simply walk down the street, the digital camera potentially has us in view. This gathering of images about us may serve legitimate ends, but clear room for abuse remains by those with regular access to these image streams or by those who gain unauthorized viewing. Those planning crimes against us or our assets can build a visual dossier concerning our daily routines, when and where we come and go, and how we are most vulnerable.

Disinformation

When someone deliberately plants information online to mislead or to deceive the public, or a specifically targeted audience, about an individual's reputation, personal life, or business that person creates disinformation. In some cases such calculated disseminating of lies becomes civil libel, an intentional attempt to harm or to ruin a person's standing. Allegations of sexual immorality, racism, abuse of others, a past criminal history, or irresponsible actions can all come into play in a disinformation campaign. The vast online apparatus of social networking sites offers many venues for propagating lies and distortions. And, no single posting needs to be "over the top." Aggregating information about individuals become fairly easy through search engines, and special aggregating sites focus on social networking. So, placing harmful information, perhaps low in intensity on a given site, gains cumulative momentum, when one aggregates the data from multiple locations and postings. And, of course, the more locations that point to something being true, the more it will be believed.

Disinformation also encompasses posting deceptions about one's business, profession, or trade. Allegations about inferior products or services, unethical business or professional practices, consumer complaints, or business problems all generate damaging impacts ranging from being a nuisance to causing grave consequences. Such deceptions are unfair practices used to malign competitors with the hope of reducing their market share. Protecting one's commercial or professional reputation online has become a serious matter.

Misuse of Electronic Surveillance

Whether we drive through a toll booth on a highway, shop in a retail store, pay a bill in person, gamble in a casino, or enter a government building, we come under electronic surveillance. In most cases this electronic record remains in benign hands and before trusted eyes. Yet, those with access to the digital record may abuse their authority. Catherine Price in "The Anonymity Experiment" (*Popular Science,* 2008) describes her attempt to live outside of the surveillance umbrella. In addition to the examples cited above, she discovered that smartphones enable GPS tracking of the user's location visible to real time on a map with the right software. Renting a car, buying a ticket

or checking in at an airport, getting married, and having a baby all can include a visual record being made. Those with access to this visual record may exploit the knowledge it offers to sell information about us. A visual chronology of our daily events and peregrinations may aid in identity theft, stealing our information, or in preparing for crimes against our persons or property.

CRIMES AGAINST PERSONS' INFORMATION ASSETS

This division of the text covers offenses such as identity theft, social engineering, the theft of personal information repositories, the theft of physical information assets, and the misuse of online information. Threats involving identity theft and social engineering get excellent coverage in the press. However, the other threats need some preliminary explanation. Personal information repositories range from USB drives to memory cards to information stored in "cloud" servers on the Internet and on mobile devices. As indicated earlier, physical information assets include rare books, manuscripts, and other paper-based records of special value or of a sensitive nature. Their inclusion in the book rests upon the fact that such assets may be overlooked in a developing an overall information security plan, and they deserve an investigator's attention when a loss occurs. The misuse of online information does not constitute always a crime per se. It is not illegal to compile a "dossier" on an individual from publicly available information. Such research or focused aggregation of data, however, can serve as a foundation for subsequent criminal activity against a target or the target's information assets.

Identity Theft

The more information about someone available online and in print, the greater the chances become for the individual to evolve into a target. Social networking sites offer fertile ground for mining information about individuals. In conducting investigations into identity thefts, an extensive interview with the victim often reveals the main points of vulnerability. Where has the victim been online? What information has he or she posted online? What social networking sites does the victim use? What printed sources are available about the victim? These