CYBERCRIME INVESTIGATORS

HANDBOOK

GRAEME EDWARDS

WILEY

Cybercrime Investigators Handbook

Cybercrime Investigators Handbook

GRAEME EDWARDS,PhD.

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993, or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Cataloging-in-Publication Data
Names: Edwards, Graeme (Financial and cybercrime investigator), author.
Title: Cybercrime investigators handbook / Graeme Edwards.
Description: Hoboken, New Jersey : John Wiley & Sons, Inc., [2020] |
Includes index.
Identifiers: LCCN 2019023231 (print) | LCCN 2019023232 (ebook) | ISBN 9781119596288 (cloth) | ISBN 9781119596325 (adobe pdf) | ISBN 9781119596301 (epub)
Subjects: LCSH: Computer crimes—Investigation.
Classification: LCC HV8079.C65 E39 2020 (print) | LCC HV8079.C65 (ebook) | DDC 363.25/968—dc23
LC record available at https://lccn.loc.gov/2019023231
LC ebook record available at https://lccn.loc.gov/201902323

Cover Design: Wiley
Cover Image: © South_agency/iStock.com

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To Marie and Bob. Long gone but not forgotten.
To Liz and the girls. Thank you for putting up with the numerous hours
I have spent on work, study, and research for this book and all the support
you have given.

Contents

List of Figures

About the Author

Dr. Graeme Edwards is a financial and cybercrime investigator located in Brisbane, Australia. He has 26 years' experience in policing, with 17 years as a detective specializing in the investigation of financial crimes and cybercrimes.

He has successfully completed a doctorate in information technology with his thesis, "Investigating Cybercrime in a Cloud-Computing Environment." He has also successfully completed a master of information technology (security).

Dr. Edwards is a regular conference presenter, speaking on a wide range of topics related to financial crimes and cybercrimes; he also conducts training events for organizations and senior management as well as undertaking post investigation analysis of cyber events. He was the president of the Brisbane chapter of the Association of Certified Fraud Examiners from 2016 to 2018.

Foreword

CYBERCRIME INVESTIGATION is a discipline relevant to an increasingly diverse audience. It's a profession that has evolved with technology and that is constantly being presented with challenges in determining the truth behind alleged events. As part of the broader cyber security profession, investigators in large part are valued for their practical experience, vendor certifications, and trustworthiness in delivering investigative outcomes—whether that be to prove or disprove alleged offending.

Graeme Edwards embodies these qualities. He forged a career as one of Australia's first true cybercrime detectives with the Queensland Police Service. Like many in our profession he took it upon himself to continue to self-develop, through learning about and adapting to new technology environments, and through advancing his own education. His doctorate furthered his expertise in cloud investigations and forensics, anticipating the growing need for this subspecialization.

Cybercrime Investigators Handbook is a life work for Graeme. It provides an opportunity for readers to directly benefit from his unique expertise and lifelong learning experiences. Its content steps readers through the investigative process from a cybercrime perspective, capturing key practical and observational gems readers can readily apply to their own challenges.

Thanks to authors like Graeme, our profession can continue to evolve and benefit from the passing on of key lessons and knowledge for the betterment of practitioners and those looking to move into the exciting field of cybercrime investigations. It's a very timely contribution. I trust you'll benefit from its content as much as I have. Thank you, Graeme, for advancing our profession in this very meaningful way.

Professor David Lacey
Managing Director, IDCARE
Director, Institute for Cyber Investigations and Forensics, USC

Acknowledgments

IT IS APPROPRIATE to thank those who have supported the writing of this book.

First, thank you to my family for putting up with the numerous hours I have spent studying, researching, and working the very antisocial hours a police officer on shift work dedicates to their profession. Without your support, this book and years of study and research would not have been achieved.

I also wish to thank Dennis Desmond, a former agent for the FBI National Computer Crime Squad in Washington, DC, and Professor Lacey, both now members of the Institute for Cyber Investigations and Forensics in Queensland, for their peer review of the contents of this book. I would also like to thank Professor Lacey for his foreword.

Cybercrime Investigators Handbook

CHAPTER ONE

1 Introduction

CYBER-ATTACKS AGAINST businesses and individuals have been occurring for decades. Many have been so successful they were never discovered by the victims and only identified while the data was being exploited or being sold on criminal markets. Cyber-attacks damage the finances and reputation of a business and cause significant damage to those whose data has been stolen and exploited.

From the criminal's perspective, the current cyber environment effectively gives them a free pass when it comes to attacking their target. They can do whatever they like to an individual or business online, cause immense damage of a professional or personal nature, and make large sums of money safe in the knowledge the complainant will rarely report the matter to police. In fact, this is a strange anomaly about cybercrime: a company has millions of dollars of intellectual property (IP) stolen from them, has all the personally identifying information (PII) of the staff and clients stolen, and the action of reporting it to police or investigating who is behind the attack is rarely considered or undertaken unless forced by local legislation. Consequently, from the criminal's perspective, there is little to no downside to being a cybercriminal. They operate on a high-financial-return, low-risk model.

Due to the high volume and complexity of cyber-attacks, should a victim decide to refer a complaint to police they cannot always rely upon them to be available to undertake an investigation and locate the offender. Police resources are stretched and skilled cyber investigators in law enforcement are few and overworked. This means organizations subject to a cyber-attack that wish to find information about who is behind the attack will need to hire an experienced cyber investigator (scarce and very expensive) or investigate the matter themselves. Alternatively, they will not conduct an investigation and instead focus on increasing security.

The decision by victims to not investigate a cybercrime is made for many reasons, including the time and money to be expended on an investigation, the focus of the business being directed on the investigation, the internal disruption it causes, and the reputational harm caused when the community finds the company security has been breached and all the data entrusted to them stolen. Also, directors would not look forward to the day that they stand before a public annual general meeting and explain to the shareholders that all the company data was stolen on their watch and that they have made no effort to recover it or identify who took it.

To the members of an incident response (IR) team or the cyber investigator, responding to an attack is often an inexact science as the attackers' motives and skill levels vary. Whereas an attack against a single desktop computer may be easily contained and investigated, an attack against a complete distributed corporate network will require significant resources and an experienced response team to protect the company, their data, and clients. As the attack methodologies vary, the investigation strategy will not necessarily follow the exact same path each time.

Investigating a cyber-attack may be a critical part of the continuation of the business. When the attack is discovered, a mixture of panic, stress, anxiety, and fear is seen among staff, and those tasked to mitigate and eradicate the attack may feel the future of the company rests upon their shoulders. Many employees will be concerned as to their personal future, as they will be familiar with the many stories of businesses hit by a cyber-attack that no longer exist six months later. Staff members of the organization being interviewed as a part of the incident response may also feel that they are being held responsible and that the interview is a method of laying blame at their feet.

So why conduct an investigation and gather evidence? Why should a company start investigating the cybercrime and try to track down the offender? With the proliferation in the instances of cybercrime, there is an expectation among the community that those who are entrusted with their PII take their responsibilities seriously and ensure their data is secure.

Shareholders of companies who find that the value of their shares and/or dividends is affected by a breach may demand efforts by the company to identify and prosecute the attacker. In the initial aftermath of the attack, there may be the possibility of locating the suspect and the digital property taken and recovering it before it is exploited. It may be argued that the duties and responsibilities of a director include trying to recover the stolen corporate data before it is exploited.

Outside of law enforcement and several large businesses, such as the major accounting companies, there are few options for those who want to have an investigation into a cyber-attack conducted. The IR team may find evidence pointing to a suspect, but it is generally not their job to prepare a case for referral to police or lawyers. A cyber investigator is a very specialized position and is roughly the equivalent of a police detective conducting a criminal investigation, as the rules of evidence the court demands are the same whether you are an experienced detective or a civilian investigator.

The cyber investigator is viewed as the person who is tasked with finding evidence of the person behind the attack, and in some cases preparing a referral to police or commencing a civil prosecution. While many attacks originate from overseas and are hidden behind multiple legal jurisdictions, anonymizers, bots, or other technology, people have their own motivations to commit crimes—and these people may include current or former employees residing within your local jurisdiction.

The role of the cyber investigator is an extension of the digital investigator. For the benefit of this book, the digital investigator is the person who conducts a forensic examination of a device or network and produces a report on the evidence seized and identified.

This book is intended for the person assigned the task of investigating the cyber event with a view to gaining a full understanding of the event and where possible recovering the IP/PII before it is exploited. They may also be tasked with finding evidence to support an action in a tribunal (e.g., employment court) or a potential prosecution in a civil or criminal court should the attacker be identified. It will also be of benefit to the manager/executive/lawyer who is tasked to review an investigation to understand the actions of the investigation team and why certain decisions were made and to gain an understanding of the evidence available from a cybercrime scene and the follow-up investigation. This is not a book that describes how to technically respond to and mitigate a cyber-attack, as there are many books covering this topic in great detail. There are also many courses offered by organizations that teach the many aspects of responding to a cyber-attack from the technical perspective.

Although this book makes some references to material from third parties, it is not intended to be an academic book. This is because much of the material is not from academic literature or web sources, but from the experience of the author as a cybercrime investigator. The major exception to this is Chapter 12, which relies on evidence from the author's doctoral thesis on cybercrime investigation in a cloud-computing environment and where academic references from a literature review are noted. Where explanations are provided, as in the glossary, they are largely kept at a low-level technical definition to allow those new to this field of work to understand the material and its relevance without having to learn a whole new language called technology.

Due to the dynamic nature of evidence, advances in technology, and the evolution of legislation/court decisions, this book is not intended to be an exclusive guide in every legal jurisdiction or to cover every potential cyber event. Where material in this book conflicts in any way with the laws of your jurisdiction, the legal environment(s) you operate in will always take precedence. The book intends, however, to provoke critical thinking among management, IR team managers, and investigators facing a complex legal and technical environment should a suspect be identified and subsequent evidence need to be presented to a tribunal or court.

This book contains many of the steps a cybercrime investigator will undertake, from the initial identification of a cyber event through to considering a prosecution in court. There are many lists of things the investigator may consider. These are not exhaustive lists and are provided to expand the thinking as to what to do, where evidence may reside, and how to legally obtain and manage it. Use this book as a prompt and not as a definitive step-by-step template, as each cyber investigation is different and each jurisdiction has its own legal requirements.

The lists in this book provide a handy point of direction in each stage of the investigation. As you will discover, at each stage there are many things to be done and no one can remember them all every time. So, the lists are provided as a memory prompt of things to consider and apply as the circumstances, legislation in your jurisdiction, and your experience dictate. Not all items in the lists will be relevant in all instances. The explanations are in plain language and technical terms are kept to a minimum to assist your understanding of new concepts.

In Chapter 2 we provide an introduction to the cybercriminal and a series of offenses an investigator may be called upon to investigate. These will vary according to the laws of the jurisdiction(s) you are operating in and terms for the offenses will vary. By gaining an understanding of the cybercriminal and their chosen cybercrimes, we gain an understanding of how the crime was committed and why it was committed in the manner it was, as well as gaining some understanding of the type of identity we are seeking.

Once we understand typical offenses, in Chapter 3 we look at the motivations of the attacker. In some instances, understanding the attacker's motives will provide a strong pointer as to who the offender is, especially in cases of internal offenses. Motivations will vary across the many forms of cyber-attack you will investigate. It is worth understanding the reasons why a criminal attacks a specific target, as this will make great sense to them, even if the motivation seems unusual to the investigator.

In Chapter 4 we will look at examples of the alerts that may be the first indicators of the cyber event, as well as the offender's methodologies. These alerts and methodologies may be evidence in their own right and provide indicators as to the identity of the offender. While an alert will be generated before the investigator is brought in, the evidence from the alert will provide direction for the investigator to use as a platform for their investigation.

In Chapter 5 we will learn the process of commencing a cybercrime investigation. We will discuss the many reasons why an investigation is commenced and introduce who a cyber investigator is. While the common response to a cyber event is to fix the system and prevent an attack from happening again, we also will ask whether there is a responsibility on the part of the data owner to identify the attacker and attempt to get the stolen data back before it is exploited.

Once we have an understanding of offenses, offenders' motivations, initial alerts, and attack methodology, in Chapter 6 we will learn about the role of the law in your investigation. Should an attacker be identified and presented before the court, every aspect of your investigation is subject to critical examination in court by the defendant's lawyers, and your actions and their legality may be as much on trial as the activity of the defendant.

Whether you are conducting a civil or criminal investigation, the complainant will provide direction to the investigation they want from you. They will have information on which to base your investigation as well as the authority to provide the resources you require. In Chapter 7 we will cover the many aspects of your initial meeting with the complainant, including numerous questions you may find relevant to ask them at this meeting.

Chapter 8 provides a general introduction to the role of the digital investigator for the cyber investigator. Although the cyber investigator will not necessarily be involved in the technical aspect of the incident response while the attack is underway, it will be of benefit to them to understand what the IR examiners are doing and the consequences of their actions involving the digital evidence.

The cyber investigator will be involved in preserving evidence and in discussion with the digital investigator and IR teams as to the seizure of evidence, including placing a priority on preserving digital evidence, especially that which is most volatile.

The cyber environment provides many unique challenges to the investigator, and a variety of these challenges are introduced in Chapter 9. As you are operating in a dynamic environment, the challenges you face will vary according to the circumstances of your case and the evidence you are seeking.

In Chapter 10 we move into the cybercrime scene investigation and cover many of the areas of a search you need to be aware of and understand. Cybercrime investigations involve unique challenges to the investigator and these are identified and discussed. As you are operating in a physical and digital environment the challenges faced will differ among investigations, and the investigator will need to expand their thinking to understand their changing environment.

Log files are critical to cybercrime investigations: when activated and secured, they will tell you a lot about the attacker, their methodologies, and the data they accessed. In Chapter 11 we will introduce many log types, where they can be found, and what they mean to you as an investigator.

Log files are like video cameras at a crime scene. They can be effective—or, like a camera, if they are turned off or output not preserved, can be totally unusable. Log record activity on a device and network may provide very valuable evidence as to what happened, how it happened, when the breach occurred, and in some instances, who was behind it. The investigator may need to work with the digital investigator to understand what the logs are saying; however, this form of technical evidence may be crucial to your investigation—to the point where you may be criticized in court if you did not follow this potential evidence trail.

Chapter 12 addresses legal and technical issues involved in locating and lawfully seizing evidence from a cloud-computing platform. As data is now stored on multiple computer servers in multiple legal jurisdictions, evidence identification and preservation has become a far more complex procedure than when the examiner could physically seize a device that was suspected of being breached. Chapter 12 covers many of the legal and technical issues to be considered by the investigator, with suggested pathways to advancing your investigation in the cloud.

Chapter 13 provides a very brief introduction to the Internet of Things (IoT), which includes the multitude of devices now connected online. Evidence may now be gathered from anywhere there is a device connected to the Internet, and the digital investigator may use this technology to support their investigation.

Open source material is material that can be captured from online sources. There are numerous forms of open source information available online and many cyber investigators are finding valuable information to support their investigations by conducting online searches. Chapter 14 introduces a sample of the many forms of open source information available and how this information can assist your inquiries.

As cybercrime has become more professional over the past decade, the criminal community has created specialized markets where they can trade goods and services with customers. Criminal markets such as Silk Road and AlphaBay obtained a great deal of publicity through identifying the manner in which members of the criminal community operate and the level of support provided to each other in training and other support mechanisms. In Chapter 15 we will introduce the dark web and discuss its relevance to the investigator, with a warning not to venture into the criminal markets unless you as an investigator are well trained and understand the environment in which you will be operating. In some jurisdictions, it is an offense to access the dark web.

Interviewing witnesses and suspects is an art that many police officers and investigators take years to master. It is not a simple process, as each interview is unique and may be evidence in its own right. Chapter 16 will discuss many of the considerations to be undertaken when conducting an interview and safeguards that may be applied depending on the jurisdiction you are operating within.

Chapter 17 discusses how to review evidence collected and provide direction as to how to proceed. Sometimes you will have strong leads to the suspect, sometimes you may have enough evidence to commence or refer an investigation, and sometimes you will be facing a dead end with a recommendation to complete your investigation.

Should you have enough evidence to refer to a tribunal, civil court, or police, Chapter 18 discusses ideas for how to prepare your evidence for court. Each jurisdiction has its own rules, and your priority will be to obtain experienced legal advice to ensure the requirements of the law and court are met. How you present your evidence is sometimes as valuable as the strength of your prosecution.

Finally, in Chapter 19 we provide a summary of the contents of the book.

A glossary is also provided. It is prepared using nontechnical language, as readers will come from many backgrounds, many of which are not technical. Its aim is to provide a very general understanding of the new terminology mentioned, so you may continue reading with an understanding of the concept and the circumstances in which it is referenced. Should you require a more technical understanding of these concepts, there are many online resources available to you.

As a prime reason cyber security exists is the cybercriminal, we commence this book with an examination of the potential criminal offenses that may be committed in a digital and cyber environment.

2

CHAPTER TWO

Cybercrime Offenses

THE POTENTIAL offenses a criminal may commit against an entity or individual is limited only by the imagination of the attacker. The cybercriminal may be a long-term trusted employee within the organization or a person located on the other side of the world. They could also be a contractor who takes advantage of operating within the corporate network to install malicious software or access information by installing a server on the network to intercept and record all traffic without the authority of the system's administrator.

This chapter seeks to present to the investigator an understanding of the many forms of cybercrime they may be required to investigate. While the investigation techniques presented in this book may be similar across each crime type, an understanding of the crime goes a long way toward understanding the criminal. This then provides direction as to where to locate digital evidence within the physical and digital crime scene as well as to understanding the criminal's motivation.

As technology evolves, so do the opportunities for the criminal community to evolve with it. As new technological products are released into the marketplace, criminals view the product or service with a view as to how it may be exploited to progress their criminal ventures. For example, when gaming consoles provided an internal hard drive to store the games as well as to provide

Internet connectivity, criminals started storing evidence of their crimes—such as Child Exploitation Material (CEM)—within the hard drive of the console, so should police conduct a search warrant at their address, they were less likely to seize a gaming console than a laptop or desktop computer. As criminals develop these skills, law enforcement reacts to them and develops their evolving field of investigative knowledge.

Cybercriminals share their knowledge on open source and closed criminal forums, resulting in a higher standard of criminal who can seek experienced assistance when their attempted crime meets a hurdle. Cybercriminals also provide tutorials for those new to the industry, including step-by-step methodologies on how to commit cybercrime without leaving behind digital evidence leading to their identity. Should it be required, some sites provide one-on-one tutorials and peer review. In essence cybercrime is a profession, with many resources available to the criminals. These same resources can also be useful to the investigator in understanding developing methodologies and the ways criminals conduct their activities.

An advantage of cybercrime to a criminal, when compared to other forms of crime, is the lack of structural complexity. When compared to a crime such as illegal drug trafficking, cybercrime lacks the structural managerial complexities that are prevalent in crimes involving physical property. A drug trafficker may be required to structure the business, distribution, processing, transporting, competition, physical threats, sales network, and money laundering. In cybercrime, there are fewer of these considerations involved. As opposed to the illegal drug trade, where parties involved maybe personally known to each other and build relationships, those involved in partnerships in cybercrime may not ever physically meet each other, assisting each other based on their areas of expertise. Also, a valuable consideration is there are no turf wars involved in cybercrime, as there are in the illegal drugs trade.[1]

There are many other reasons why cybercrime is attractive to the criminal. One of these is the financial reward available compared to other forms of crime. Joseph Schafer and his colleagues found that on average the bank robber may obtain $2,500, the bank fraudster $25,000, and the cybercriminal $250,000. They also found that the cost of the theft of technology to an organization is approximately $1.9 million.[2]

Alongside the financial rewards, a further attraction of cybercrime to the criminal is that the actions required are easy to carry out and hard to detect. The Internet provides anonymity for skilled cybercriminals, who use available technological resources (such as free web-based email accounts). Schafer and his colleagues found that the anonymity cybercriminals are operating under