1 Introduction
The Need for Good Cybercrime Investigators

This chapter (and book) is for:

- You
- Law enforcement of all types: police, investigators, agents, prosecutors, analysts
- Those in the private sector investigating or dealing with cybercrime
- Regulators
- The technically skilled and those who are not
- Beginning cyber investigators, intermediate, and even experienced looking for a comprehensive view
- Lawyers and non-lawyers.

At the start of each chapter, we will identify the type of cybercrime investigator for whom that chapter is primarily intended. Cybercrime investigators do not just have the title of "investigator". They come from many jobs and backgrounds – lawyers and non-lawyers; technical experts and technical beginners; experienced traditional investigators who are learning about cybercrime, and investigators whose only experience is with cybercrime; law enforcement agents, industry regulators, and members of the private sector; and students and trainees just starting out. Given this diversity of backgrounds, we recognize that some readers might read the book straight through, and some might skip chapters because they are working on a time-sensitive matter, or because existing skill sets make certain chapters less critical. That said, we think you will get something out of every chapter.

1.1 WHY THIS BOOK

Let us start with three fundamental truths about investigating cybercrime:

1. *We all can investigate cybercrime.* Cybercriminals are running amok online partly because of the misconception that only specialized investigators with vast technological resources can work these cases. Tech skills and gadgets are great to have, but they are, by no means, a requirement for handling a cyber investigation.

2. *Cybercrime can be solved*. Just because it is a cybercrime, doesn't mean it is hard to solve. Cybercriminals – like every type of criminal – run the gamut, from low-level scammers to highly sophisticated organizations. They are not all tech-wizards. They are not all hard to find.
3. *Even the most sophisticated cybercriminals can be caught*.

Bottom line: the common preconception that cybercrime is too difficult to investigate is wrong. Every case can and should be investigated. Every investigator can take positive steps to solve a case. Instead of looking at a cyber incident and assuming there is not much that can be done, we can use these core truths about cybercrime to frame a plan of action.

Cybercrime is a relatively new phenomenon. Malicious actors no longer need to be in the immediate vicinity of their victims, but can attack and steal remotely, even from abroad. The reach of the Internet means cybercrime is a safety and security problem for every community, industry, business, and law enforcement agency – large or small.

Investigating cybercrime is an even newer endeavor than cybercrime itself, and because it involves technology, it can seem daunting to many investigators and victims. How do you start investigating when one of these incidents happens? How do you figure out who did it when the perpetrator is hiding online? What do you do with a crime that seems to lead across the country, let alone around the world?

When we first started working on cybercrime cases as prosecutors, we had the same questions. We did not come to this work from a tech background, and we often had minimal resources available. But through time, effort, and creativity we learned how to find the answers. We learned that cybercrime can be investigated, offenders can be found, and cases can be successfully prosecuted.

We wrote this book to share this knowledge with you, and to inspire more people to become cybercrime investigators – especially those who might think cybercrime is too challenging to take on.

We understand that, in some places, law enforcement and private security lack experience, training, and resources when it comes to cybercrime. That is another reason we wrote this book. We want to give any interested investigator the knowledge and tools to handle these cases. As cybercrime continues to grow, we need more investigators on the frontlines ready, willing and able to take it on. There are concrete steps that every investigator can take to tackle cybercrime. This book is designed to make these steps understandable and doable for investigators everywhere.

Why is it so important to bolster the investigative response to cybercrime? Let's look at some of the major repercussions of cybercrime in today's world.

- *Profit and Losses*. Cybercrime is immensely profitable for cybercriminals, but immensely costly to the rest of us. Each year, U.S. businesses and consumers lose billions of dollars through cybercrime while the criminal and private investigation of these events remains completely inadequate. It is astonishing to consider that billions of dollars can be stolen annually without proper investigation or redress.
- *Terrorism and Espionage*. The profitable and disruptive nature of cybercrime means it is an activity of interest for terrorists and nation-states seeking income, intelligence, or simply a new way to inflict harm. The Internet provides a gateway and a network for all manner of nefarious activity at the local, national, and international levels. Our will to investigate this activity must measure up to the threat it presents.
- *New Ways to Move Money*. Cybercriminals have developed innovative money laundering techniques to pay each other and disguise their illicit income. Virtual currencies and cryptocurrencies, international wire transfer schemes, money held and

moved in stored-value cards (like gift cards), criminal proceeds funneled through multiplayer video games – these are some of the methods cybercriminals use, along with more traditional money laundering mechanisms. Once proven successful, these techniques are adopted not just by cyber thieves, but by other criminals looking to conduct illicit transactions, such as child pornographers, narcotics dealers, and terrorists.

- *Stalking, Revenge, and Harassment*. Stealing is not the only form of cybercrime – the Internet is used to commit a wide variety of crimes meant to harass, stalk, menace, or otherwise target specific individuals. The increasingly sophisticated methods used to conduct these crimes are capable of inflicting tremendous, ongoing harm to victims. The scenarios range from teen sexting to cyber-revenge acts directed at employers, intimate partners, and political figures – and often require a response from a combination of law enforcement and private sector investigators.
- *Civil Liability and Regulation*. The scourge of cybercrime has an enormous impact on both our civil law and regulatory systems. When cybercriminals steal funds or data, injured victims may use the civil legal system to seek redress, including for cybersecurity negligence. Government regulators create and enforce rules that deal with the real threats that cybercrime presents to sensitive data and online commerce.

This book discusses all of these topics, and many other pressing issues around cybercrime, in a manner designed to help every kind of investigator find useful information.

1.2 WHO INVESTIGATES CYBERCRIME?

Cybercrime creates many types of victims, and its ripple effects have led to an intense focus on cybersecurity, information security, and privacy. As a result, cybercrime is investigated for a variety of reasons. To provide information in the most effective way throughout this book, we considered the needs and concerns of investigators representing these three important groups:

- *Law Enforcement*

Law enforcement, including police, federal law enforcement, and prosecutors, receive thousands of cybercrime reports every year from individual and corporate victims. When state and local police investigate cybercrimes, along with prosecutors, it is usually because they get the first calls when local residents are victimized. Traditionally, more complex cases are tackled by federal law enforcement agencies (such as the FBI, U.S. Secret Service, and Department of Homeland Security) and federal prosecutors. These agencies use monetary thresholds and other criteria to take on a select number of investigations. Some state Attorney General's offices also handle "bigger" cybercrime cases. A few local District Attorneys' (DA) offices handle significant cybercrime cases, as we did while working at the Manhattan DA's office. But the truth is, the vast majority of cybercrimes go uninvestigated.

One of this book's goals is to change the way investigators look at cyber cases. Historically, investigators have categorized cases too quickly as being "local" or "small", only realizing, after some investigation, that they are really one piece of a larger scheme. Nowadays, all police agencies, whether an enormous department like the New York City Police Department, or a small-town force with fewer than 20 sworn officers, will be called upon to take a cybercrime complaint and conduct an initial investigation – actions that may lead to uncovering larger, additional crimes. Since these investigations normally require prosecutorial assistance, it is essential that prosecutors in local DAs' offices also know how to

investigate cybercrime. As we explain in this book, when a "small" case turns out to be part of a big scheme, there are many choices investigators can make about how to proceed – including identifying and collaborating with agencies that have the resources to assist with or take on a broader investigation. Of course, the objective is always to better investigate, identify, and prosecute those responsible for cybercrime.

- *Regulators and State Attorneys General*

Not all investigations of cybercrime are conducted for the purpose of criminal prosecution. Federal regulators and state Attorneys General investigate cybercrime to determine whether consumer protection laws have been violated, or to ensure compliance with industry regulations. These regulatory investigations often focus on specific aspects of cybercrime that fall under the agencies' authority – such as ensuring private sector compliance with cybersecurity, privacy, and data breach notification laws, or taking legal action when companies fail to comply with laws or regulations.

- *Private Sector*

Many cybercrime investigations are undertaken by individuals and businesses who fall victim to cybercrime, then want to know how it happened, who was responsible, and what has to be done to prevent further harm. An increasing number of these investigations are prompted by laws and regulations that require victimized businesses to investigate and report cybercrime, including financial institutions, health care services, and businesses of all sizes.

The goals of a private sector investigation may diverge from those of law enforcement and government regulators. For example, businesses damaged by cybercrime may be concerned about how to apportion legal responsibility among themselves for settlement or insurance purposes. Even when law enforcement conducts an investigation, private entities may investigate as well. At times, private sector resources and access to information can greatly assist law enforcement, providing benefits to both groups.

Private sector investigations might be conducted in-house or might require the hiring of specialized firms or individuals. The decision about who should investigate within the private sector depends upon the size of the organization, circumstances, and resources.

1.3 HOW THIS BOOK IS ORGANIZED

This book is organized into four parts.

Part I: Understanding Cybercrime, Computers, and Cybersecurity
Part II: Law for the Cybercrime Investigator
Part III: The Cybercrime Investigation
Part IV: Litigation: Cybercrime Investigations in Court

In Part I, we present chapters with essential background knowledge for understanding cybercrime. We cover criminal activities that can be called a "cybercrime" – including the most prevalent types of online schemes and who commits them. We also introduce computers, networks, digital forensics, and information security. For those who are concerned they are unqualified to investigate cybercrime because of a lack of such expertise, these chapters are a primer that will help you get up to speed on some of the technological terms and actions that might come up in a cyber investigation.

In Part II, we review the laws and rules about cybercrime and gathering evidence. It is hard to conduct an investigation if you do not know what facts might be relevant and how the legal process might play out. First, we provide an introduction to criminal and civil law. Our intention here is to demystify central legal concepts and explain them in straightforward terms. Next, we look at the criminal statutes defining cybercrime. There is no "crime" in cybercrime unless there is a statute prohibiting an act; thus, an important part of a successful criminal investigation is focusing on the correct criminal charges to pursue. Then, we examine the tools used by law enforcement to find and collect evidence of cybercrimes, while describing the restrictions our legal system imposes to protect privacy and regulate government action. We also discuss the civil and regulatory implications of cybercrime, as government and business face increasing regulatory and security standards for handling cyber threats. Part II includes an overview of cyber actions committed by nation-states or terrorists, recognizing that some investigations may reveal these national cyber threats.

Part III focuses on conducting a cyber investigation. After first looking at the broader objectives and strategies of any cyber investigation, we devote individual chapters to investigations performed within the private sector, by law enforcement, and by regulators. This part also provides in-depth discussion of some of the key investigative methods and stages in a cyber investigation – including the cyclical investigative process, open-source investigation, obtaining records and analyzing them, investigations into financial activity and money laundering, uncovering cybercriminals' true identities, and locating and apprehending suspects once they are identified (within the United States and internationally).

Part IV explains how a cyber investigation plays out in the context of litigation. From the perspectives of both criminal and civil cases, we look at how an investigator's methods and results are presented and dissected in court. Knowing how an investigation might eventually be used in litigation can enable better investigative decision-making.

1.4 KEEPING IT FUN: ANECDOTES, CASES, DIAGRAMS, AND CARTOONS

Throughout the book, we work to keep the material lively and interesting, by using:

A thread case. We give real-life examples of the many investigative topics covered in the book by weaving through the chapters our "thread case", the Western Express case we both prosecuted. The phases and events from this investigation provide real-world examples of how some of these legal and investigative concepts can be applied.

Western Express Example Text Box

The Western Express case involved the indictment, arrest and prosecution of 17 defendants from all around the United States and four other countries. It centered on a vast cyber money-laundering operation used to hide the proceeds from the theft, sale, and use of tens of thousands of stolen credit and debit card account profiles.

Anecdotes. We also include interesting anecdotes throughout the text, including several from our years spent as Manhattan prosecutors.

Cartoons and diagrams. The text of the book is illustrated by numerous diagrams and cartoons. We offer these visual aids in order to present complex concepts in a digestible format and to make the material easier to remember. As they say, a picture is worth a thousand words, as depicted in Figure 1.1.

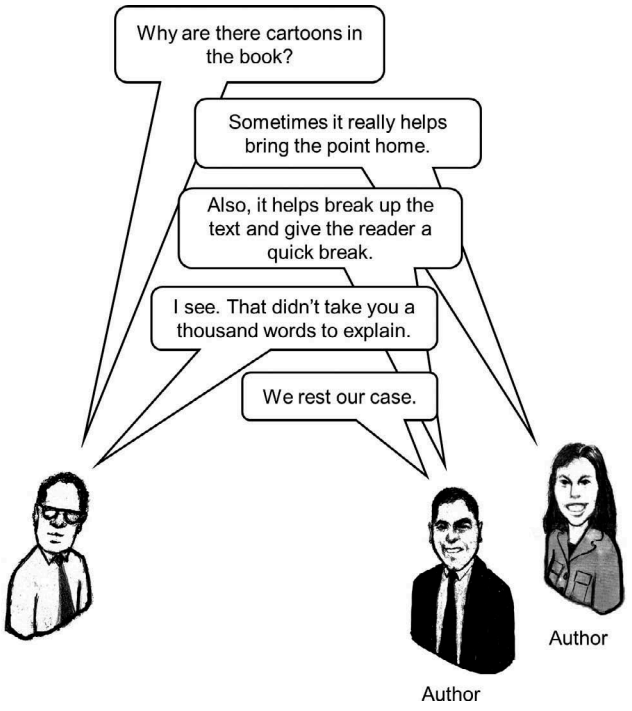

FIGURE 1.1 Cartoon Example.

1.5 ONWARD AND UPWARD

Most importantly, we hope you have as much fun reading this book as we had writing it!