LEARNING MADE EASY

Cybersecurity

for dummies®

A Wiley Brand

- Evaluate possible cybersecurity threats
- Protect your family and business against potential breaches
- Identify the steps for recovery after a cyber attack

Joseph Steinberg

Cybersecurity

by Joseph Steinberg

for dummies®
A Wiley Brand

Cybersecurity For Dummies®

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Published simultaneously in Canada

ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit https://hub.wiley.com/community/support/dummies.

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 Control Number: 2019948325

ISBN 978-1-119-56032-6 (pbk); ISBN 978-1-119-56035-7 (ePDF); ISBN 978-1-119-56034-0 (epub)

Cybersecurity For Dummies®

To view this book's Cheat Sheet, simply go to www.dummies.com and search for "Cybersecurity For Dummies Cheat Sheet" in the Search box.

Table of Contents

List of Illustrations

Chapter 2

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 11

Chapter 14

List of Tables

Chapter 13

Chapter 15

Introduction

In the course of just a single generation, the world has undergone some of the greatest changes since the dawn of mankind. The availability of the Internet as a tool for consumers and businesses alike, coupled with the invention of mobile devices and wireless networking, have ushered in an Information Revolution that has impacted just about every aspect of human existence.

This reliance on technology, however, has also created enormous risks. It seems that not a day goes by without some new story emerging of a data breach, cyberattack, or the like. Simultaneously, because humanity's reliance on technology increases on a daily basis, the potential adverse consequences of cyberattacks have grown exponentially to the point that people can now lose their fortunes, their reputations, their health, or even their lives, as the result of cyberattacks.

It is no wonder, therefore, that people living in the modern world understand the need to protect themselves from cyber-dangers. This book shows you how to do so.

About This Book

While many books have been written over the past couple decades on a wide variety of cybersecurity-related topics, most of them don't provide the general population with the information needed to properly protect themselves.

Many cybersecurity books are directed toward highly technical audiences and tend to overwhelm noncomputer scientists with extraneous information, creating severe challenges for readers seeking to translate the knowledge that they acquire from books into practical actions. On the flip side, various self-published introduction-to-cybersecurity books suffer from all sorts of serious deficiencies, including, in some cases, having been written by non-experts and presenting significant amounts of misinformation. Anyone interested in

cybersecurity often shouldn't trust these materials. Likewise, many security tip sheets and the like simply relay oft-repeated clichés and outdated advice, sometimes causing people who follow the recommendations contained within such works to worsen their cybersecurity postures rather than improve them. Furthermore, the nearly constant repetition of various cybersecurity advice by media personalities after news stories about breaches ("Don't forget to reset all your passwords!"), coupled with the lack of consequences to most people after they do not comply with such directives, has led to *cybersecurity fatigue* — a condition in which folks simply don't act when they actually need to because they have heard the "boy cry wolf" one too many times.

I wrote *Cybersecurity For Dummies* to provide people who do not work as cybersecurity professionals with a foundational book that can teach them what they need to know about cybersecurity and explain why they need to know it. This book offers you practical, clear, and straightforward advice that you can easily translate into actions that can help keep you and your children, parents, and small businesses cybersecure.

Cybersecurity For Dummies is divided into several parts. Parts 1, 2, and 3 provide an overview of cybersecurity and give tips on protecting yourself and your loved ones from both external threats and from making dangerous (and potentially disastrous) mistakes. Topics such as how to secure your online accounts and how to select and protect passwords fall into these parts of the book.

Part 4 offers tips on securing small businesses, which may be especially pertinent for small business owners and employees. Part 4 then also discusses some of the unique security needs that face firms as they grow larger and touches on cybersecurity-in-government related matters.

Part 5 shows you how to identify security breaches. Part 6 covers the process of backing up, something that you should do proactively before the need to recover arises, as well as how to recover from security breaches.

Part 7 looks toward the future — both for those interested in potentially pursuing a cybersecurity-related career (or who have children or other relatives or friends considering doing so) as well as those interested in how emerging technologies are likely to impact their own personal cybersecurity.

Part 8 gives several lists of ten items that you may want to keep as tip sheets.

Please keep in mind that while internalizing all the information in this book, and putting it into practice, will likely dramatically improve your cybersecurity posture, reading this book will no more make you an expert in cybersecurity than reading a book on the workings of the human heart will quickly transform you into a competent cardiologist.

Cybersecurity is a complex, rapidly changing field whose professionals spend years, if not decades, studying and working full-time to develop, sharpen, and maintain the skills and expertise that they utilize on a constant basis. As such, please do not consider the advice within this book as a substitute for hiring a professional for any situation that reasonably warrants the latter.

Also, please keep in mind that technical products change quite often, so any screenshots included within the book may not be identical to the screens that you observe when you perform similar actions to those described in the text. Remember: Cybersecurity threats are constantly evolving, as are the technologies and approaches utilized to combat them.

Foolish Assumptions

In this book, I make some assumptions about your experience with technology:

- You have experience with using a keyboard and pointer, such as a mouse, on either a Mac or Windows PC and have access to one of those machines.

- You know how to use an Internet browser, such as Firefox, Chrome, Edge, Opera, or Safari.
- You know how to install applications on your computer.
- You know how to perform a Google search.

Conventions Used in This Book

As you explore each part of this book, keep the following points in mind:

- Words that are being defined appear in *italic*.
- Code and URLs (web addresses) are shown in `monofont`.

Icons Used in This Book

Throughout the margin of this book are small images, known as icons. These icons mark important tidbits of information:

TIP The Tip icon identifies places where I offer additional tips for making this journey more interesting or clear. Tips cover some neat shortcuts that you may not have known about.

REMEMBER The Remember icon bookmarks important points that you'll want to keep in mind.

WARNING The Warning icon helps protect you from common errors and may even give you tips to undo your mistakes.

Beyond This Book

In addition to what you're reading right now, this product also comes with a free access-anywhere Cheat Sheet that covers important cybersecurity actions. To get this Cheat Sheet, simply go to www.dummies.com and search for *Cybersecurity For Dummies Cheat Sheet* in the Search box.

Where to Go from Here

Cybersecurity For Dummies is designed in such a fashion that you don't have to read the book in order or even read the entire book.

If you purchased this book because you suffered a cybersecurity breach of some sort, for example, you can skip to the Part 5 without reading the prior material (although reading it afterwards may be wise, as it may help you prevent yourself from becoming the victim of another cyberattack).

Part 1

Getting Started with Cybersecurity

IN THIS PART …

Discover what cybersecurity is and why defining it is more difficult than you might expect.

Find out why breaches seem to occur so often and why technology alone does not seem to stop them.

Explore various types of common cyberthreats and common cybersecurity tools.

Understand the who, how, and why of various types of attackers and threatening parties that aren’t officially malicious.

Chapter 1

What Exactly Is Cybersecurity?

IN THIS CHAPTER

- **Understanding that cybersecurity means different things for different entities**
- **Clarifying the difference between cybersecurity and information security**
- **Showing why cybersecurity is a constantly moving target**
- **Understanding the goals of cybersecurity**
- **Looking at the risks mitigated by cybersecurity**

To improve your ability to keep yourself and your loved ones cybersecure, you need to understand what cybersecure means, what your goals should be vis-à-vis cybersecurity, and what exactly you're securing against.

While the answers to these questions may initially seem simple and straightforward, they aren't. As you can see in this chapter, these answers can vary dramatically between people, company divisions, organizations, and even within the same entity at different times.

Cybersecurity Means Different Things to Different Folks

While *cybersecurity* may sound like a simple enough term to define, in actuality, from a practical standpoint, it means quite different things to different people in different situations, leading to extremely varied relevant policies, procedures, and practices. An individual who wants to protect her social media accounts from hacker takeovers, for example, is

exceedingly unlikely to assume many of the approaches and technologies used by Pentagon workers to secure classified networks.

Typically, for example:

- For **individuals,** *cybersecurity* means that their personal data is not accessible to anyone other than themselves and others whom they have so authorized, and that their computing devices work properly and are free from malware.
- For **small business owners,** *cybersecurity* may include ensuring that credit card data is properly protected and that standards for data security are properly implemented at point-of-sale registers.
- For **firms conducting online business,** *cybersecurity* may include protecting servers that untrusted outsiders regularly interact with.
- **For shared service providers,** *cybersecurity* may entail protecting numerous data centers that house numerous servers that, in turn, host many virtual servers belonging to many different organizations.
- For the **government,** *cybersecurity* may include establishing different classifications of data, each with its own set of related laws, policies, procedures, and technologies.

REMEMBER The bottom line is that while the word cybersecurity is easy to define, the practical expectations that enters peoples' minds when they hear the word vary quite a bit.

Technically speaking, cybersecurity is the subset of information security that addresses information and information systems that store and process data in electronic form, whereas *information security* encompasses the security of all forms of data (for example, securing a paper file and a filing cabinet).

That said, today, many people colloquially interchange the terms, often referring to aspects of information security that are technically not part of cybersecurity as being part of the latter. Such usage also results from

the blending of the two in many situations. Technically speaking, for example, if someone writes down a password on a piece of paper and leaves the paper on his desk where other people can see the password instead of placing the paper in a safe deposit box or safe, he has violated a principle of information security, not of cybersecurity, even though his actions may result in serious cybersecurity repercussions.

Cybersecurity Is a Constantly Moving Target

While the ultimate goal of cybersecurity may not change much over time, the policies, procedures, and technologies used to achieve it change dramatically as the years march on. Many approaches and technologies that were more than adequate to protect consumers' digital data in 1980, for example, are effectively worthless today, either because they're no longer practical to employ or because technological advances have rendered them obsolete or impotent.

While assembling a complete list of every advancement that the world has seen in recent decades and how such changes impact cybersecurity in effectively impossible, we can examine several key development area and their impacts on the ever-evolving nature of cybersecurity: technological changes, economic model shifts, and outsourcing.

Technological changes

Technological changes tremendously impact cybersecurity. New risks come along with the new capabilities and conveniences that new offerings deliver. As the pact of technological advancement continues to increase, therefore, so does the pace of new cybersecurity risks. While the number of such risks created over the past few decades as the result of new offerings is astounding, the areas described in the following sections have yielded a disproportionate impact on cybersecurity.

Digital data

The last few decades have witnessed dramatic changes in the technologies that exist, as well as vis-à-vis who use such technologies, how they do so, and for what purposes. All these factors impact cybersecurity.

Consider, for example, that when many of the people alive today were children, controlling access to data in a business environment simply meant that the data owner placed a physical file containing the information into a locked cabinet and gave the key to only people he recognized as being authorized personnel and only when they requested the key during business hours. For additional security, he may have located the cabinet in an office that was locked after business hours and which itself was in a building that was also locked and alarmed.

Today, with the digital storage of information, however, simple filing and protection schemes have been replaced with complex technologies that must automatically authenticate users who seek the data from potentially any location at potentially any time, determine whether the users are authorized to access a particular element or set of data, and securely deliver the proper data — all while preventing any attacks against the system servicing data requests, any attacks against the data in transit, and any of the security controls protecting the both of them.

Furthermore, the transition from written communication to email and chat has moved tremendous amounts of sensitive information to Internet-connected servers. Likewise, society's move from film to digital photography and videography has increased the stakes for cybersecurity. Nearly every photograph and video taken today is stored electronically rather than on film and negatives — a situation that has enabled criminals situated anywhere to either steal people's images and leak them, or to hold people's valuable images ransom with ransomware. The fact that movies and television shows are now stored and transmitted electronically has likewise allowed pirates to copy them and offer them to the masses — sometimes via malware-infested websites.

The Internet

The most significant technological advancement when it comes to cybersecurity impact has been the arrival of the Internet era. Just a few

decades ago, it was unfathomable that hackers from across the globe could disrupt a business, manipulate an election, or steal a billion dollars. Today, no knowledgeable person would dismiss any such possibilities.

Prior to the Internet era, it was extremely difficult for the average hacker to financially profit by hacking. The arrival of online banking and commerce in the 1990s, however, meant that hackers could directly steal money or goods and services — which meant that not only could hackers quickly and easily monetize their efforts, but unethical people had strong incentives to enter the world of cybercrime.

Cryptocurrency

Compounding those incentives severalfold has been the arrival and proliferation of cryptocurrency over the past decade, along with innovation that has dramatically magnified the potential return-on-investment for criminals involved in cybercrime, simultaneously increasing their ability to earn money through cybercrime and improving their ability to hide while doing so. Criminals historically faced a challenge when receiving payments since the account from which they ultimately withdrew the money could often be tied to them. Cryptocurrency effectively eliminated such risks.

Mobile workforces and ubiquitous access

Not that many years ago, in the pre-Internet era, it was impossible for hackers to access corporate systems remotely because corporate networks were not connected to any public networks, and often had no dial-in capabilities. Executives on the road would often call their assistants to check messages and obtain necessary data while they were remote.

Connectivity to the Internet created some risk, but initially firewalls did not allow people outside the organization to initiate communications — so, short of firewall misconfigurations and/or bugs, most internal systems remained relatively isolated. The dawn of e-commerce and e-banking, of course, meant that certain production systems had to be

reachable and addressable from the outside world, but employee networks, for example, usually remained generally isolated.

The arrival of remote access technologies — starting with services like Outlook Web Access and pcAnywhere, and evolving to full VPN and VPN-like access — has totally changed the game.

Smart devices

Likewise, the arrival of smart devices and the *Internet of Things (*the universe of devices that are not traditional computers, but that are connected to the Internet) — whose proliferation and expansion are presently occurring at a startling rate — means that unhackable solid-state machines are being quickly replaced with devices that can potentially be controlled by hackers halfway around the world. The tremendous risks created by these devices are discussed more in Chapter 17.

Big data

While big data is helping facilitate the creation of many cybersecurity technologies, it also creates opportunities for attackers. By correlating large amounts of information about the people working for an organization, for example, a criminal can more easily than before identify ideal methods for social engineering his/her way into the organization or locate and exploit possible vulnerabilities in the organization's infrastructure. As a result, various organizations have been effectively forced to implement all sorts of controls to prevent the leaking of information.

Entire books have been written on the impact of technological advancement. The main point to understand is that technological advancement has had a significant impact on cybersecurity, making security harder to deliver and raising the stakes when parties fail to properly protect their assets.

Social shifts

Various changes in the ways that humans behave and interact with one another have also had a major impact on cybersecurity. The Internet, for example, allows people from all over the world to interact in real-time.

Of course, this real-time interaction also enables criminals all over the world to commit crimes remotely. But it also allows citizens of repressive countries and free countries to communicate, creating opportunities for dispelling the perpetual propaganda utilized as excuses for the failure of totalitarianism to produce quality of lives on par with the democratic world. At the same time, it also delivers to the cyberwarriors of governments at odds with one another the ability to launch attacks via the same network.

The conversion of various information management systems from paper to computer, from isolated to Internet-connected, and from accessible-only-in-the-office to accessible from any smartphone or computer has dramatically changed the equation when it comes to what information hackers can steal. Furthermore, in many cases in which such conversions were, for security reasons, not initially done, the pressure emanating from the expectations of modern people that every piece of data be available to them at all times from anywhere has forced such conversions to occur, creating additional opportunities for criminals. To the delight of hackers, many organizations that, in the past, wisely protected sensitive information by keeping it offline have simply lost the ability to enjoy such protections if they want to stay in business.

Social media has also transformed the world of information — with people growing accustomed to sharing far more about themselves than ever before — often with audiences far larger than before as well. Today, due to the behavioral shift in this regard, it is trivial for evildoers from anywhere to assemble lists of a target's friends, professional colleagues, and relatives and to establish mechanisms for communication with all those people. Likewise, it is easier than ever before to find out what technologies a particular firm utilizes and for what purposes, discover people's travel schedules, and ascertain their opinions on various topics or their tastes in music and movies. The trend toward increased sharing continues. Most people remain blindly unaware of how much information about them lives on Internet-connected machines and how much other information about them can be extrapolated from the aforementioned data.

All these changes have translated into a scary reality: Due to societal shifts, an evildoer can easily launch a much larger, more sophisticated social engineering attack today than he or she could less than a decade ago.

Economic model shifts

Connecting nearly the entire world has allowed the Internet to facilitate other trends with tremendous cybersecurity ramifications. Operational models that were once unthinkable, such as that of an American company utilizing a call center in India and a software development shop in the Philippines, have become the mainstay of many corporations. These changes, however, create cybersecurity risks of all sorts.

The last 20 years have seen a tremendous growth in the outsourcing of various tasks from locations in which they're more expensive to carry out to regions in which they can be accomplished at much lower costs. The notion that a company in the United States could rely primarily on computer programmers in India or in the Philippines or that someone in New York seeking to have a logo made for her business could, shortly before going to bed, pay someone halfway around the globe $5.50 to create it and have the logo in her email inbox immediately upon waking up the next morning, would have sounded like economic science-fiction a generation ago. Today, it's not only common, but also in many cases, it is the more common than any other method of achieving similar results.

Of course, many cybersecurity ramifications result. Data being transmitted needs to be protected from destruction, modification, and theft, and greater assurance is needed that back doors are not intentionally or inadvertently inserted into code. Greater protections are needed to prevent the theft of intellectual property and other forms of corporate espionage. Hackers no longer necessarily need to directly breach the organizations that they seek to hack; they merely need to compromise one or more of its providers, which may be far less careful with their information security and personnel practices than the ultimate target.

Political shifts

As with advances in technology, political shifts have had tremendous cybersecurity repercussions, some of which seem to permanent fixtures of news headlines. The combination of government power and mighty technology has often proven to be a costly one for citizens. If current trends continue, the impact on cybersecurity of various political shifts will only continue to grow in the foreseeable future.

Data collection

The proliferation of information online and the ability to attack machines all over the world have meant that governments can spy on citizens of their own countries and on the residents of other nations to an extent never before possible.

Furthermore, as more and more business, personal, and societal activities leave behind digital footprints, governments have easy access to a much greater amount of information about their potential intelligence targets than they could acquire even at much higher costs just a few years ago. Coupled with the relatively low cost of digital storage, advancing big data technologies, and the expected eventual impotence of many of today's encryption technologies, and governments have a strong incentive to collect and store as much data as they can about as many people as they can, in case it is of use at some later date. There is little doubt that some governments are already doing exactly that.

The long-term consequences of this phenomenon are, obviously, as of yet unknown, but one thing is clear: If businesses do not properly protect data, less-than-friendly nations are likely to obtain it and store it for use in either the short term, the long term, or both.

Election interference

A generation ago, one nation interfering in the elections of another was no trivial matter. Of course, such interference existed — it has occurred as long as there have been elections — but carrying out significant interference campaigns was expensive, resource-intensive, and risky.

To spread misinformation and other propaganda, materials had to be printed and physically distributed or recorded and transmitted via radio, meaning that individual campaigns were likely to reach only small

audiences. As such, the efficacy effects of such efforts were often quite low, and the risk of the party running the campaign being exposed was relatively high.

Manipulating voter registration databases to prevent legitimate voters from voting and/or to allow bogus voters to vote was extremely difficult and entailed tremendous risks; someone “working on the inside” would likely have had to be a traitor. In a country such as the United States, in which voter registration databases are decentralized and managed on a county level, recruiting sufficient saboteurs to truly impact a major election would likely have been impossible, and the odds of getting caught while attempting to do so were likely extremely high. Likewise, in the era of paper ballots and manual counting, for a foreign power to manipulate actual vote counts on any large scale was practically impossible.

Today, however, the game has changed. A government can easily spread misinformation through social media at an extremely low cost. If it crafts a well-thought-out campaign, it can rely on other people to spread the misinformation — something that people could not do en masse in the era of radio recordings and printed pamphlets. The ability to reach many more people, at a much lower cost than ever before, has meant that more parties are able to interfere in political campaigns and can do so with more efficacy than in the past. Similarly, governments can spread misinformation to stir up civil discontent within their adversaries nations and to spread hostility between ethnic and religious groups living in foreign lands.

With voter registration databases stored electronically and sometimes on servers that are at least indirectly connected to the Internet, records may be able to be added, modified, or deleted from halfway across the globe without detection. Even if such hacking is, in reality, impossible, the fact that many citizens today believe that it may be possible has led to an undermining of faith in elections, a phenomenon that we have witnessed in recent years and that has permeated throughout all levels of society. Even Jimmy Carter, a former president of the United States, has expressed that he believes that full investigation into the 2016

presidential election would show that Donald Trump lost the election — despite there being absolutely no evidence whatsoever to support such a conclusion, even after a thorough FBI investigation into the matter.

It is also not hard to imagine that if online voting were ever to arrive, the potential for vote manipulation by foreign governments, criminals, and even political parties within the nation voting — and for removing the ballot auditability that exists today — would grow astronomically.

Less than a decade ago, the United States did not consider election-related computer systems to be critical infrastructure and did not directly provide federal funding to secure such systems. Today, most people understand that the need for cybersecurity in such areas is of paramount importance, and the policies and behavior of just a few years ago seems nothing short of crazy.

Hacktavism

Likewise, the spread of democracy since the collapse of the Soviet Union a generation ago, coupled with Internet-based interaction between people all over the globe, has ushered in the era of hacktivism. People are aware of the goings-on in more places than in the past. Hackers angry about some government policy or activity in some location may target that government or the citizens of the country over which it rules from places far away.

Greater freedom

At the same time, repressed people are now more aware of the lifestyles of people in freer and more prosperous countries, a phenomenon that has both forced some governments to liberalize, and motivated others to implement cybersecurity-type controls to prevent using various Internet-based services.

Sanctions

Another political ramification of cybersecurity has been vis-à-vis international sanctions: Rogue states subject to such sanctions have been able to use cybercrime of various forms to circumvent the sanctions.

For example, North Korea is believed to have spread malware that mines cryptocurrency for the totalitarian state to computers all over the world, thereby allowing the country to circumvent sanctions by obtaining liquid money that can easily be spent anywhere.

In 2019, the failure by individuals to adequately secure their personal computers can directly impact political negotiations.

Creating a new balance of power

While the militaries of certain nations have long since grown more powerful than those of their adversaries — both the quality and quantity of weapons vary greatly between nations — when it comes to cybersecurity the balance of power is totally different.

While the quality of cyberweapons may vary between countries, the fact that launching cyberattacks costs little means that all militaries have an effectively unlimited supply of whatever weapons they use. In fact, in most cases, launching millions of cyberattacks costs little more than launching just one.

Also, unlike in the physical world in which any nation that bombed civilian homes in the territory of its adversary may face a severe reprisal, rogue governments regularly hack with impunity people in other countries. Victims often are totally unaware that they have been compromised, rarely report such incidents to law enforcement, and certainly don’t know whom to blame.

Even when a victim realizes that a breach has occurred and even when technical experts point to the attackers as the culprits, the states behind such attacks often enjoy plausible deniability, preventing any government from publicly retaliating. In fact, the difficulty of ascertaining the source of cyberattacks coupled with the element of plausible deniability is a strong incentive for governments to use cyberattacks as a mechanism of proactively attacking an adversary, wreaking various forms of havoc without fear of significant reprisals.

Furthermore, the world of cybersecurity created a tremendous imbalance between attackers and defenders that works to the advantage of less powerful nations.

Governments that could never afford to launch huge barrages against an adversary in the physical world can easily do so in the world of cyber, where launching each attack costs next to nothing. As a result, attackers can afford to keep attacking until they succeed — and they need to breach systems only once to "succeed" — creating a tremendous problem for defenders who must shield their assets against every single attack. This imbalance has translated into a major advantage for attackers over defenders and has meant that even minor powers can successfully breach systems belonging to superpowers.

In fact, this imbalance contributes to the reason why cybersecurity breaches seem to occur so often, as many hackers simply keep attacking until they succeed. If an organization successfully defends against 10 million attacks but fails to stop the 10,000,001, it may suffer a severe breach and make the news. Reports of the breach likely won't even mention the fact that it has a 99.999999 percent success rate in protecting its data and that it successfully stopped attackers one million times in a row. Likewise, if a business installed 99.999 percent of the patches that it should have but neglected to fix a single known vulnerability, it's likely to suffer a breach due to the number of exploits available to criminals. Media outlets will point out the organization's failure to properly patch, overlooking its near perfect record in that area.

As such, the era of cyber has also changed the balance of power between criminals and law enforcement.

Criminals know that the odds of being caught and successfully prosecuted for a cybercrime are dramatically smaller than those for most other crimes, and that repeated failed attempts to carry out a cybercrime are not a recipe for certain arrest as they are for most other crimes. They are also aware that law enforcement agencies lack the resources to pursue the vast majority of cyber criminals. Tracking down, taking into custody, and successfully prosecuting someone stealing data from halfway across the world via numerous hops in many countries and a network of computers commandeered from law-abiding folks, for example, requires gathering and dedicating significantly more resources

than does catching a thief who was recorded on camera while holding up in a store in a local police precinct.

With the low cost of launching repeated attacks, the odds of eventual success in their favor, the odds of getting caught and punished miniscule, and the potential rewards growing with increased digitalization, criminals know that cybercrime pays, underscoring the reason that you need to protect yourself.

Looking at the Risks That Cybersecurity Mitigates

People sometimes explain the reason that cybersecurity is important as being "because it prevent hackers from breaking into systems and stealing data and money." But such a description dramatically understates the role that cybersecurity plays in keeping the modern home, business, or even world running.

In fact, the role of cybersecurity can be looked at from a variety of different vantage points, with each presenting a different set of goals. Of course the following lists aren't complete, but they should provide food for thought and underscore the importance of understanding how to cybersecure yourself and your loved ones.

The goal of cybersecurity: The CIA triad

Cybersecurity professionals often explain that the goal of cybersecurity is to ensure the Confidentiality, Integrity, and Availability (CIA) of data, sometimes referred to as the CIA Triad, with the pun lovingly intended:

- **Confidentiality** refers to ensuring that information isn't disclosed or in any other way made available to unauthorized entities (including people, organizations, or computer processes).

WARNING Don’t confuse confidentiality with privacy: Confidentiality is a subset of the realm of privacy. It deals specifically with protecting data from unauthorized viewers, whereas privacy in general encompasses much more.

Hackers that steal data undermine confidentiality.

- **Integrity** refers to ensuring that data is both accurate and complete.

  Accurate means, for example, that the data is never modified in any way by any unauthorized party or by a technical glitch. *Complete* refers to, for example, data that has had no portion of itself removed by any unauthorized party or technical glitch.

  Integrity also includes ensuring *nonrepudiation*, meaning that data is created and handled in such a fashion that nobody can reasonably argue that the data is not authentic or is inaccurate.

  Cyberattacks that intercept data and modify it before relaying it to its destination — sometimes known as *man-in-the-middle attacks* — undermine integrity.

- **Availability** refers to ensuring that information, the systems used to store and process it, the communication mechanisms used to access and relay it, and all associated security controls function correctly to meet some specific benchmark (for example, 99.99 percent uptime). People outside of the cybersecurity field sometimes think of availability as a secondary aspect of information security after confidentiality and integrity. In fact, ensuring availability is an integral part of cybersecurity. Doing so, though, is sometimes more difficult than ensuring confidentiality or integrity. One reason that this is true is that maintaining availability often requires involving many more noncybersecurity professionals, leading to a “too many cooks in the kitchen” type challenge, especially in larger organizations. Distributed denial-of-service attacks attempt to undermine availability. Also, consider that attacks often use large numbers of stolen computer power and bandwidth to launch DDoS attacks, but responders who seek to ensure availability can only

leverage the relatively small amount of resources that they can afford.

From a human perspective

The risks that cybersecurity addresses can also be thought of in terms better reflecting the human experience:

- **Privacy risks:** Risks emanating from the potential loss of adequate control over, or misuse of, personal or other confidential information.
- **Financial risks:** Risks of financial losses due to hacking. Financial losses can include both those that are direct — for example, the theft of money from someone's bank account by a hacker who hacked into the account — and those that are indirect, such as the loss of customers who no longer trust a small business after the latter suffers a security breach.
- **Professional risks:** Risks to one's professional career that stem from breaches. Obviously, cybersecurity professionals are at risk for career damage if a breach occurs under their watch and is determined to have happened due to negligence, but other types of professionals can suffer career harm due to a breach as well. C-level executives can be fired, Board members can be sued, and so on. Professional damage can also occur if hackers release private communications or data that shows someone in a bad light — for example, records that a person was disciplined for some inappropriate action, sent an email containing objectionable material, and so on.
- **Business risks:** Risks to a business similar to the professional risks to an individual. Internal documents leaked after breach of Sony Pictures painted various the firm in a negative light vis-à-vis some of its compensation practices.
- **Personal risks:** Many people store private information on their electronic devices, from explicit photos to records of participation in activities that may not be deemed respectable by members of their respective social circles. Such data can sometimes cause significant

harm to personal relationships if it leaks. Likewise, stolen personal data can help criminals steal people’s identities, which can result in all sorts of personal problems.

Chapter 2

Getting to Know Common Cyberattacks

IN THIS CHAPTER

- **Exploring attacks that can inflict damage**
- **Discovering the difference between impersonation, data interception, and data theft**
- **Looking at the various types of malware, poisoning, and malvertising**
- **Understanding how cyberattackers exploit the challenges of maintaining complex technology infrastructures**
- **Finding out about forms of advanced cyberattacks**

Many different types of cyberattacks exist — so many that I could write an entire series of books about them. In this book, however, I do not cover all types of threats in detail because the reality is, that you're likely reading this book to learn about how to keep yourself cybersecure, not to learn about matters that have no impact on you, such as forms of attacks that are normally directed at espionage agencies, industrial equipment, or military armaments.

In this chapter, you find out about the different types of problems that cyberattackers can create through the use of attacks that commonly impact individuals and small businesses.

Attacks That Inflict Damage

Attackers launch some forms of cyberattacks with the intent to inflict damage to victims. The threat posed by such attacks is not that a

criminal will directly steal your money or data, but that the attackers will inflict harm to you in some other specific manner — a manner that may ultimately translate into financial, military, political, or other benefit to the attacker and (potentially) damage of some sort to the victim.

Types of attacks that inflict damage include

- Denial-of-service (DoS) attacks
- Distributed denial-of-service (DDoS) attacks
- Botnets and zombies
- Data destruction attacks

Denial-of-service (DoS) attacks

A *denial-of-service attack* is one in which an attacker intentionally attempts to paralyze a computer or computer network by flooding it with large amounts of requests or data, which overload the target and make it incapable of responding properly to legitimate requests.

In many cases, the requests sent by the attacker are each, on their own, legitimate — for example, a normal request to load a web page.

In other cases, the requests aren't normal requests. Instead, they leverage knowledge of various protocols to send requests that optimize, or even magnify, the effect of the attack.

In any case, denial-of-service attacks work by overwhelming computer systems' Central Processing Units (CPU)s and/or memory, utilizing all the available network communications bandwidth, and/or exhausting networking infrastructure resources such as routers.

Distributed denial-of-service (DDoS) attacks

A *Distributed DoS attack* is a DoS attack in which many individual computers or other connected devices across disparate regions simultaneously flood the target with requests. In recent years, nearly all major denial-of-service attacks have been distributed in nature — and some have involved the use of Internet-connected cameras and other

devices as attack vehicles, rather than classic computers. Figure 2-1 illustrates the anatomy of a simple DDoS attack.

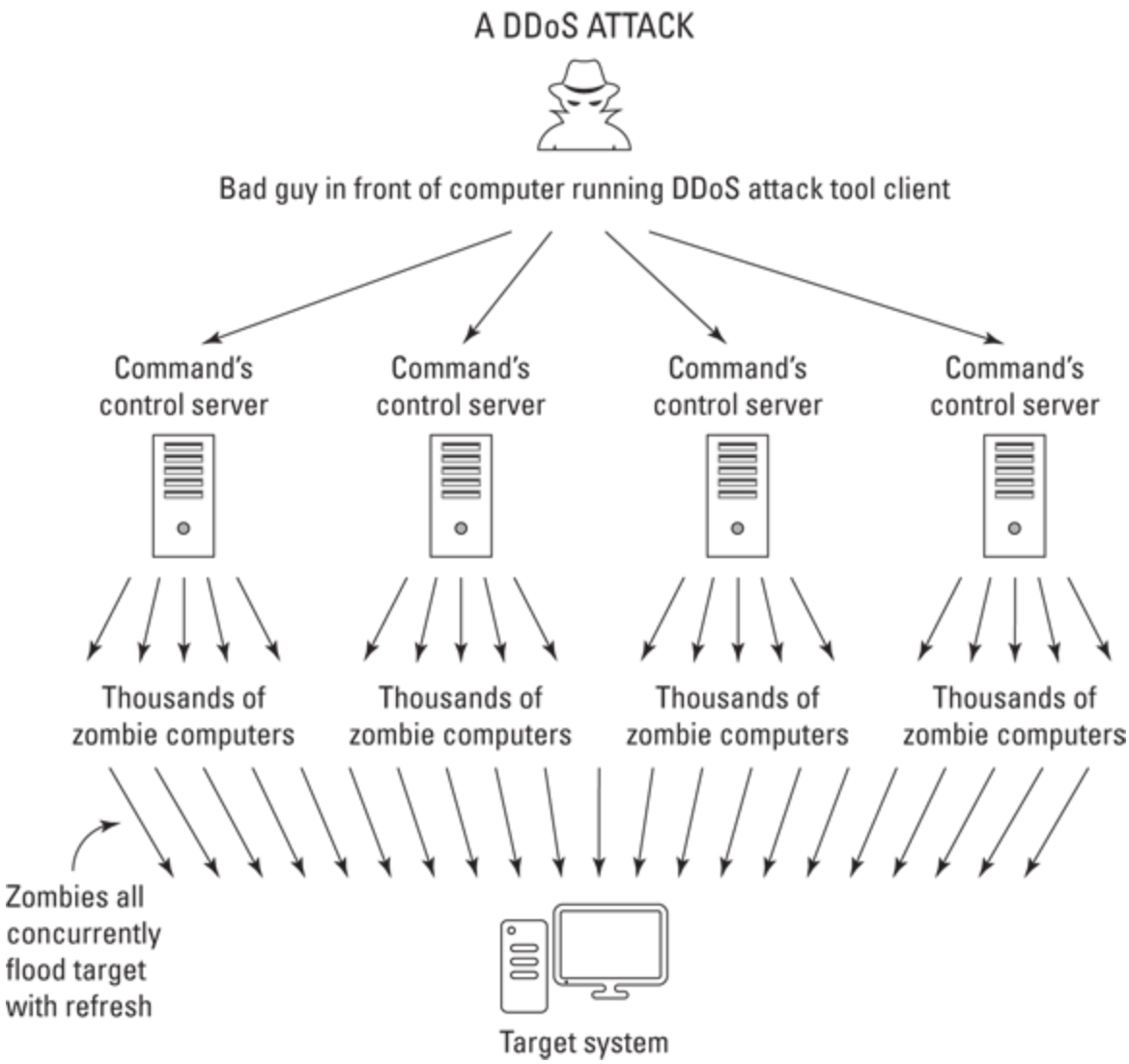

FIGURE 2-1: A DDoS attack.

The goal of a DDoS attack is to knock the victim offline, and the motivation for doing so varies.

Sometimes the goal is financial: Imagine, for example, the damage that may result to an online retailer's business if an unscrupulous competitor knocked the former's site offline during Black Friday weekend. Imagine a crook who shorts the stock of a major retailer of toys right before launching a DDoS attack against the retailer two weeks before Christmas.

DDoS attacks remain a serious and growing threat. Criminal enterprises even offer DDoS for hire services, which are advertised on the dark web as offering, for a fee, to "take your competitor's websites offline in a cost-effective manner."

In some cases, DDoS launchers may have political, rather than financial, motives. For example, a corrupt politician may seek to have his or her opponent's website taken down during an election season, thereby reducing the competitor's ability to spread messages and receive online campaign contributions. Hacktivists may also launch DDoS attacks in order to take down sites in the name of "justice" — for example, targeting law enforcement sites after an unarmed person is killed during an altercation with police.

In fact, according to a 2017 study by Kaspersky Lab and B2B International, almost half of companies worldwide that experienced a DDoS attack suspect that their competitors may have been involved.

DDoS attacks can impact individuals in three significant ways:

- **A DDoS attack on a local network can significantly slow down all Internet access from that network.** Sometimes these attacks make connectivity so slow that connections to sites fail due to *session timeout* settings, meaning that the systems terminate the connections after seeing requests take longer to elicit responses than some maximum permissible threshold.
- **A DDoS attack can render inaccessible a site that a person plans on using.** On October 21, 2016, for example, many users were unable to reach several high-profile sites, including Twitter, PayPal, CNN, HBO Now, The Guardian, and dozens of other popular sites, due to a massive DDoS attack launched against a third party providing various technical services for these sites and many more.

TIP The possibility of DDoS attacks is one of the reasons that you should never wait until the last minute to perform an online banking transaction — the site that you need to utilize may be inaccessible for a number of reasons, one of which is an ongoing DDoS attack.

- **A DDoS attack can lead users to obtain information from one site instead of another.** By making one site unavailable, Internet users looking for specific information are likely to obtain it from another site — a phenomenon that allows attackers to either spread misinformation or prevent people from hearing certain information or vantage points on important issues. As such, DDoS attacks can be used as an effective mechanism — at least over the short term — for censoring opposing points of view.

Botnets and zombies

Often, DDoS attacks use what are known as *botnets*. Botnets are a collection of compromised computers that belong to other parties, but that a hacker remotely controls and uses to perform tasks without the legitimate owners' knowledge.

Criminals who successfully infect one million computers with malware can, for example, potentially use those machines, known as *zombies*, to simultaneously make many requests from a single server or server farm in an attempt to overload the target with traffic.

Data destruction attacks

Sometimes attackers want to do more than take a party temporarily offline by overwhelming it with requests — they may want to damage the victim by destroying or corrupting the target's information and/or information systems. A criminal may seek to destroy a user's data through a *data destruction attack* — for example, if the user refuses to pay a ransomware ransom that the crook demands.

Of course, all the reasons for launching DDoS attacks (see preceding section) are also reasons that a hacker may attempt to destroy someone's data as well.

Wiper attacks are advanced data destruction attacks in which a criminal uses malware to wipe the data on a victim's hard drive or SSD, in such a fashion that the data is difficult or impossible to recover.

To put it simply, unless the victim has backups, someone whose computer is wiped by a wiper is likely to lose access to all the data and software that was previously stored on the attacked device.

Impersonation

One of the great dangers that the Internet creates is the ease with which mischievous parties can impersonate others. Prior to the Internet era, for example, criminals could not easily impersonate a bank or a store and convince people to hand over their money in exchange for some promised rate of interest or goods. Physically mailed letters and later telephone calls became the tools of scammers, but none of those earlier communication techniques ever came close to the power of the Internet to aid criminals attempting to impersonate law-abiding parties.

Creating a website that mimics the website of a bank, store, or government agency is quite simple and can sometimes be done within minutes. Criminals can find a near-endless supply of domain names that are close enough to those of legitimate parties to trick some folks into believing that a site that they are seeing is the real deal when it's not, giving crooks the typical first ingredient in the recipe for online impersonation.

WARNING Sending an email that appears to have come from someone else is simple and allows criminals to perpetrate all sorts of crimes online. I myself demonstrated over 20 years ago how I could defeat various defenses and send an email that was delivered to recipients

on a secure system — the message appeared to readers to have been sent from god@heaven.sky. Figure 2-2 shows another email message that may have been faked.

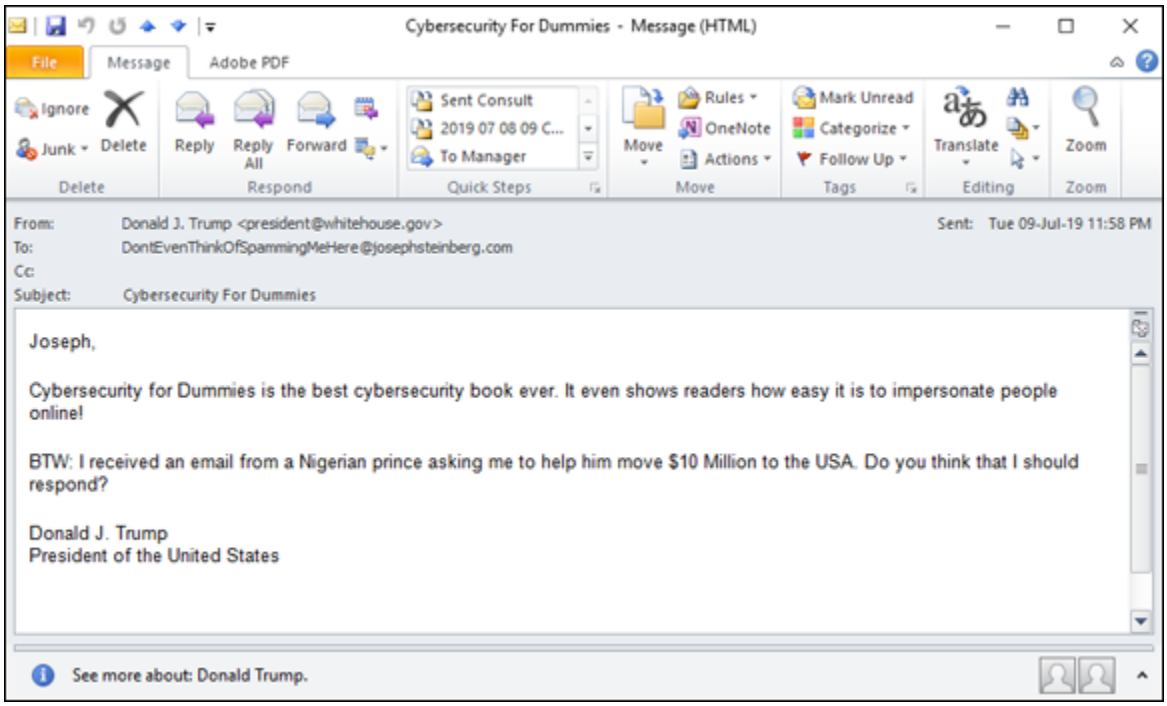

FIGURE 2-2: An impersonation message.

Phishing

Phishing refers to an attempt to convince a person to take some action by impersonating a trustworthy party that reasonably may legitimately ask the user to take such action.

For example, a criminal may send an email that appears to have been sent by a major bank and that asks the recipient to click on a link in order to reset his or her password due to a possible data breach. When the user clicks the link, he or she is directed to a website that appears to belong to the bank, but is actually a replica run by the criminal. As such, the criminal uses the fraudulent website to collect usernames and passwords to the banking site.

Spear phishing

Spear phishing refers to phishing attacks that are designed and sent to target a specific person, business, or organization. If a criminal seeks to obtain credentials into a specific company's email system, for example, he or she may send emails crafted specifically for particular targeted individuals within the organization. Often, criminals who spear phish research their targets online and leverage overshared information on social media in order to craft especially legitimate-sounding emails.

For example, the following type of email is typically a lot more convincing than "Please login to the mail server and reset your password.":

> *"Hi, I am going to be getting on my flight in ten minutes. Can you please login to the Exchange server and check when my meeting is? For some reason, I cannot get in. You can try to call me by phone first for security reasons, but, if you miss me, just go ahead, check the information, and email it to me — as you know that I am getting on a flight that is about to take off."*

CEO fraud

CEO fraud is similar to spear phishing (see preceding section) in that it involves a criminal impersonating the CEO or other senior executive of a particular business, but the instructions provided by "the CEO" may be to take an action directly, not to log in to a system, and the goal may not be to capture usernames and passwords or the like.

The crook, for example, may send an email to the firm's CFO instructing her or him to issue a wire payment to a particular new vendor or to send all the organization's W2 forms for the year to a particular email address belonging to the firm's accountant. See Figure 2-3.

CEO fraud often nets significant returns for criminals and makes employees who fall for the scams appear incompetent. As a result, people who fall prey to such scams are often fired from their jobs.

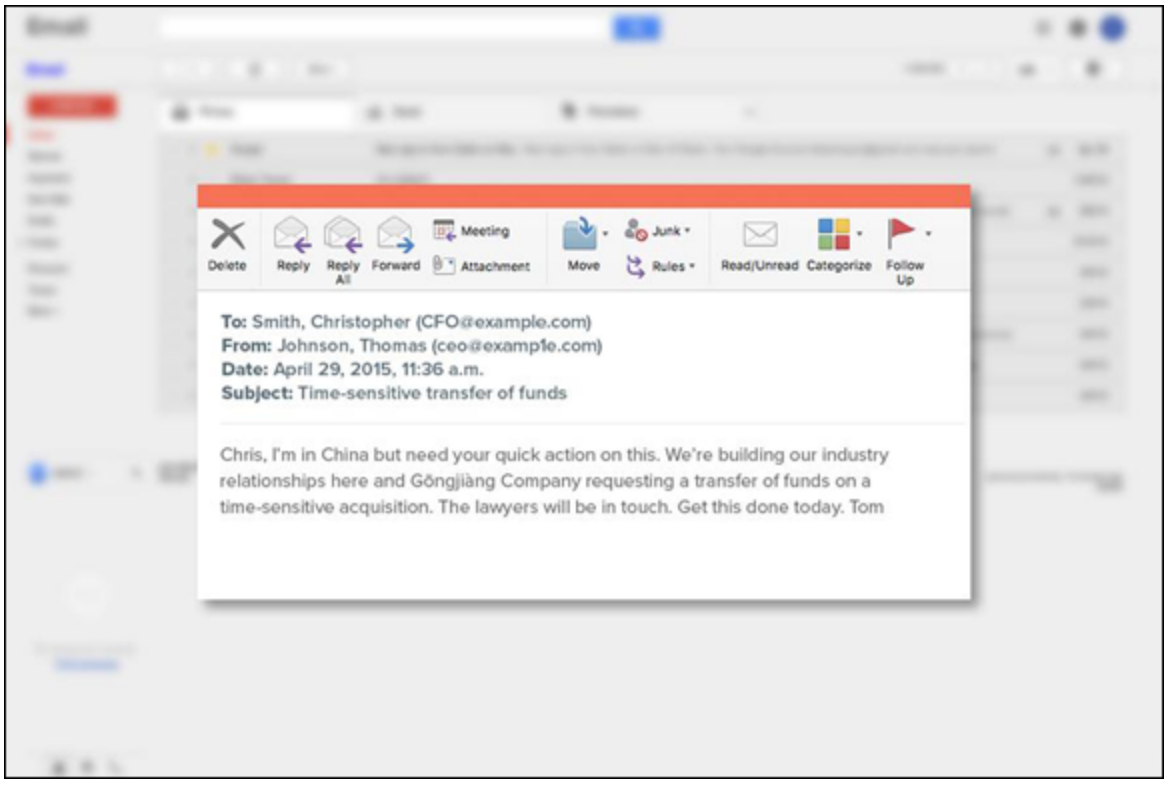

FIGURE 2-3: A fraudulent email.

Smishing

Smishing refers to cases of phishing in which the attackers deliver their messages via text messages (SMS) rather than email. The goal may be to capture usernames and passwords or to trick the user into installing malware.

Vishing

Vishing, or voice-based phishing, is phishing via POTS — that stands for "plain old telephone service." Yes, criminals use old, time-tested methods for scamming people. Today, most such calls are transmitted by Voice Over IP systems, but, in the end, the scammers are calling people on regular telephones much the same way that scammers have been doing for decades.

Whaling

Whaling refers to spear phishing that targets high-profile business executives or government officials. For more on spear phishing, see the

section earlier in this chapter.

Tampering

Sometimes attackers don't want to disrupt an organization's normal activities, but instead seek to exploit those activities for financial gain. Often, crooks achieve such objectives by manipulating data in transit or as it resides on systems of their targets in a process known as *tampering*.

In a basic case of tampering with data in transit, for example, imagine that a user of online banking has instructed his bank to wire money to a particular account, but somehow a criminal intercepted the request and changed the relevant routing and account number to his own.

A criminal may also hack into a system and manipulate information for similar purposes. Using the previous example, imagine if a criminal changed the payment address associated with a particular payee so that when the Accounts Payable department makes an online payment, the funds are sent to the wrong destination (well, at least it is wrong in the eyes of the payer).

Interception

Interception occurs when attackers capture information in transit between computers. If the data isn't properly encrypted, the party intercepting it may be able to misuse it.

One special type of interception is known as a *man-in-the-middle attack*. In this type of an attack, the interceptor proxies the data between the sender and recipient in an attempt to disguise the fact that the data is being intercepted. *Proxying* in such a case refers to the man-in-the-middle intercepting requests and then transmitting them (either in modified form or unmodified) to their original intended destinations and then receiving the responses from those destination and transmitting them (in modified form or unmodified) back to the sender. By employing proxying, the man-in-the-middle makes it difficult for the sender to know that his communications are being intercepted because

when he communicates with a server, he receives the responses that he expects.

For example, a criminal may set up a bogus bank site (see the earlier "Phishing" section) and relay any information that anyone enters on the bogus site to the actual bank site so that the criminal can respond with the same information that the legitimate bank would have sent. Proxying of this sort not only helps the criminal avoid detection — a user who provides the crook with his or her password and then performs his or her normal online banking tasks may have no idea that anything abnormal occurred during the online banking session — but, also helps the criminal ensure that he or she captures the right password. If a user enters an incorrect password, the criminal will know to prompt for the correct one.

Figure 2-4 shows the anatomy of a man-in-the-middle intercepting and relaying communications.

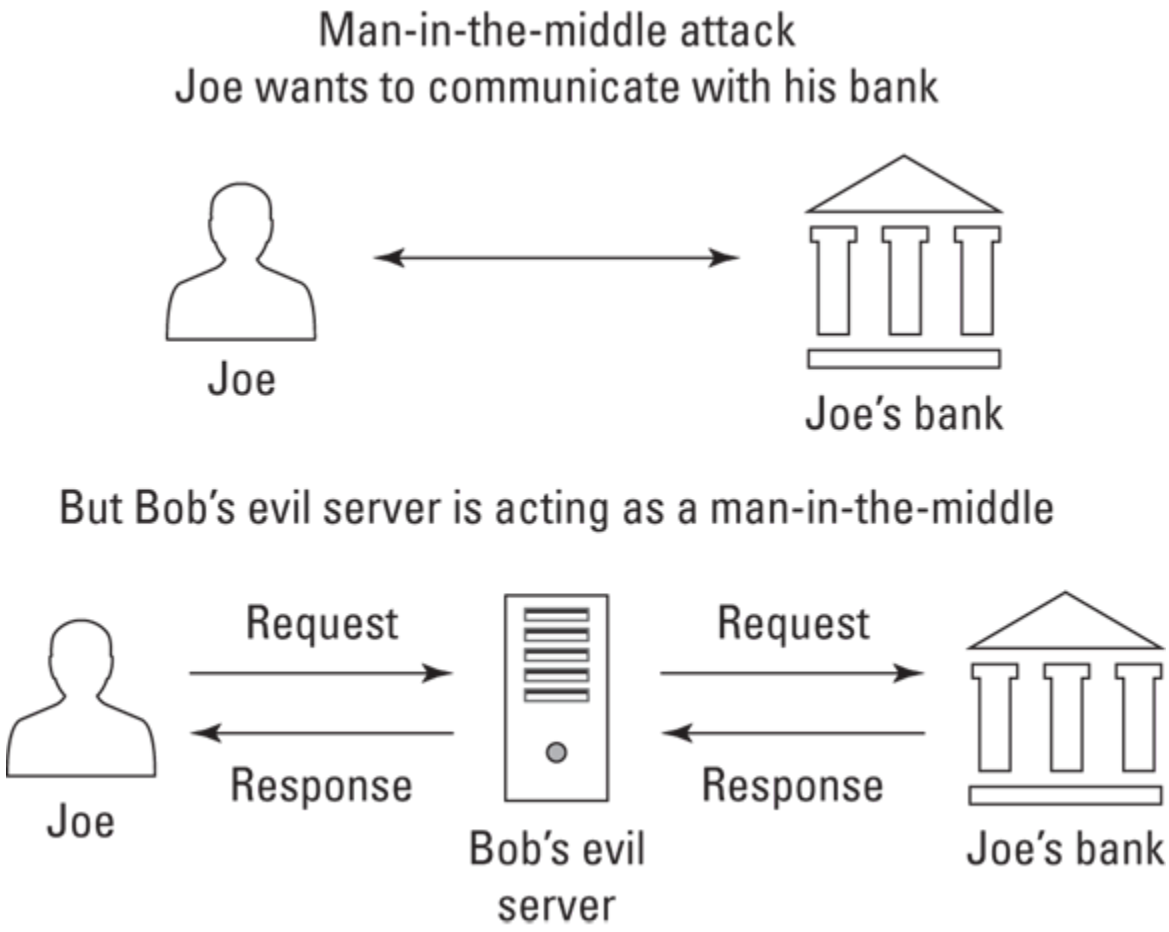

FIGURE 2-4: A man-in-the-middle interception.

Data Theft

Many cyberattacks involve stealing the victim's data. An attacker may want to steal data belonging to individuals, businesses, or a government agency for one or more of many possible reasons.

People, businesses, nonprofits, and governments are all vulnerable to data theft.

Personal data theft

Criminals often try to steal people's data in the hope of finding items that they can monetize, including:

- Data that can be used for identity theft or sold to identity thieves

- Compromising photos or health-related data that may be sellable or used as part of blackmail schemes
- Information that is stolen and then erased from the user's machine that can be ransomed to the user
- Password lists that can be used for breaching other systems
- Confidential information about work-related matters that may be used to make illegal stock trades based on insider information
- Information about upcoming travel plans that may be used to plan robberies of the victim's home

Business data theft

Criminals can use data stolen from businesses for a number of nefarious purposes:

- **Making stock trades:** Having advance knowledge of how a quarter is going to turn out gives a criminal insider information on which he or she can illegally trade stocks or options and potentially make a significant profit.
- **Selling data to unscrupulous competitors:** Criminals who steal sales pipeline information, documents containing details of future products, or other sensitive information can sell that data to unscrupulous competitors or to unscrupulous employees working at competitors whose management may never find out how such employees suddenly improved their performance.
- **Leaking data to the media:** Sensitive data can embarrass the victim and cause its stock to decline (perhaps after selling short some shares).
- **Leaking data covered by privacy regulations:** The victim may be potentially fined.
- **Recruiting employees:** By recruiting employees or selling the information to other firms looking to hire employees with similar skills or with knowledge of competitions' systems, criminals who steal emails and discover communication between employees that

indicates that one or more employees are unhappy in their current positions can sell that information to parties looking to hire.

- **Stealing and using intellectual property:** Parties that steal the source code for computer software may be able to avoid paying licensing fees to the software's rightful owner. Parties that steal design documents created by others after extensive research and development can easily save millions of dollars — and, sometimes, even billions of dollars — in research and development costs. For more on the effects of this type of theft, see the nearby sidebar "How a cyberbreach cost one company $1 billion without 1 cent being stolen."

HOW A CYBERBREACH COST ONE COMPANY $1 BILLION WITHOUT 1 CENT BEING STOLEN

Theft of intellectual property (IP), such as confidential design documents and computer source code, is an extremely serious matter and a growing area of cybercrime.

For example, in 2007, the Massachusetts-based technology firm American Superconductor, which manufactured software to control wind turbines, partnered with Sinovel, a Chinese firm that manufactured wind turbines, to start selling the turbines in China.

In 2011, Sinovel suddenly refused to pay American Superconductor $70 million that it owed the firm and began to sell turbines with its own software. An investigation revealed that Sinovel had illegally obtained the IP of American Superconductor by bribing a single employee at the American firm to help it steal the source code.

American Superconductor nearly went bankrupt as a result, declined in value by more than $1 billion, and had to let go of 700 employees, nearly half of its workforce.

Malware

Malware, or malicious software, is an all-encompassing term for software that intentionally inflicts damage on its users who typically have no idea that they are running it.

Malware includes computer viruses, worms, Trojans, ransomware, scareware, spyware, cryptocurrency miners, adware, and other programs intended to exploit computer resources for nefarious purposes.

Viruses

Computer viruses are instances of malware that, when executed, replicate by inserting their own code into computer systems. Typically, the insertion is in data files (for example, as rogue macros within a Word document), the special portion of hard drives or solid state drives that contain the code and data used to boot a computer or disk (also known as *boot sectors*), or other computer programs.

Like biological viruses, computer viruses can't spread without having hosts to infect. Some computer viruses significantly impact the performance of their hosts, while others are, at least at times, hardly noticeable.

While computer viruses still inflict tremendous damage worldwide, the majority of serious malware threats today arrive in the form of worms and Trojans.

Worms

Computer worms are stand-alone pieces of malware that replicate themselves without the need for hosts in order to spread. Worms often propagate over connections by exploiting security vulnerabilities on target computers and networks.

Because they normally consume network bandwidth, worms can inflict harm even without modifying systems or stealing data. They can slow down network connections — and few people, if any, like to see their internal and Internet connections slow down.

Trojans

Trojans (appropriately named after the historical Trojan horse) is malware that is either disguised as nonmalicious software or hidden within a legitimate, nonmalicious application or piece of digital data.

Trojans are most often spread by some form of social engineering — for example, by tricking people into clicking on a link, installing an app, or running some email attachment. Unlike viruses and worms, Trojans typically don't self-propagate using technology — instead, they rely on the effort (or more accurately, the mistakes) of humans.

Ransomware

Ransomware is malware that demands that a ransom be paid to some criminal in exchange for the infected party not suffering some harm.

Ransomware often encrypts user files and threatens to delete the encryption key if a ransom isn't paid within some relatively short period of time, but other forms of ransomware involve a criminal actually stealing user data and threatening to publish it online if a ransom is not paid.

Some ransomware actually steals the files from users' computers, rather than simply encrypting data, so as to ensure that the user has no possible way to recover his or her data (for example, using an anti-ransomware utility) without paying the ransom.

Ransomware is most often delivered to victims as a Trojan or a virus, but has also been successfully spread by criminals who packaged it in a worm. In recent years sophisticated criminals have even crafted targeted ransomware campaigns that leverage knowledge about what data is most valuable to a particular target and how much that target can afford to pay in ransoms.

Figure 2-5 shows the ransom demand screen of WannaCry — a flavor of ransomware that inflicted at least hundreds of millions of dollars in damage (if not billions), after initially spreading in May 2017. Many security experts believe that the North Korean government or others working for it created WannaCry, which, within four days, infected hundreds of thousands of computers in about 150 countries.

FIGURE 2-5: Ransomware demanding ransom.

Scareware

Scareware is malware that scares people into taking some action. One common example is malware that scares people into buying security software. A message appears on a device that the device is infected with some virus that only a particular security package can remove, with a link to purchase that "security software."

Spyware

Spyware is software that surreptitiously, and without permission, collects information from a device. Spyware may capture a user's keystrokes (in which case it is called a *keylogger*), video from a video camera, audio from a microphone, screen images, and so on.

It is important to understand the difference between spyware and invasive programs. Some technologies that may technically be considered spyware if users had not been told that they were being

tracked online are in use by legitimate businesses; they may be invasive, but they are not malware. These types of *nonspyware that also spies* includes beacons that check whether a user loaded a particular web page and tracking cookies installed by websites or apps. Some experts have argued that any software that tracks a smartphone's location while the app is not being actively used by the device's user also falls into the category of *nonspyware that also spies* — a definition that would include popular apps, such as Uber.

Cryptocurrency miners

Cryptocurrency miners are malware that, without any permission from devices' owners, commandeers infected devices' brainpower (its CPU cycles) to generate new units of a particular cryptocurrency (which the malware gives to the criminals operating the malware) by completing complex math problems that require significant processing power to solve.

The proliferation of cryptocurrency miners exploded in 2017 with the rise of cryptocurrency values. Even after price levels subsequently dropped, the miners are still ubiquitous as once criminals have invested in creating the miners, there is little cost in continuing to deploy them. Not surprisingly, as cryptocurrency prices began to rise again in 2019, new strains of cryptominers began to appear as well — some of which specifically target Android smartphones.

Many low-end cybercriminals favor using cryptominers. Even if each miner, on its own, pays the attacker very little, miners are easy to obtain and directly monetize cyberattacks without the need for extra steps (such as collecting a ransom) or the need for sophisticated command and control systems.

Adware

Adware is software that generates revenue for the party operating it by displaying online advertisements on a device. Adware may be malware — that is, installed and run without the permission of a device's owner — or it may be a legitimate component of software (for example,

installed knowingly by users as part of some free, ad-supported package).

TIP Some security professionals refer to the former as *adware malware*, and the latter as adware. Because no consensus exists, it's best to clarify which of the two is being discussed when you hear someone mention just the generic term adware.

Blended malware

Blended malware is malware that utilizes multiple types of malware technology as part of an attack — for example, combining features of Trojans, worms, and viruses.

Blended malware can be quite sophisticated and often stems from skilled attackers.

Zero day malware

Zero day malware is any malware that exploits a vulnerability not previously known to the public or to the vendor of the technology containing the vulnerability, and is, as such, often extremely potent.

Regularly creating zero day malware requires significant resource and development. It's quite expensive and is often crafted by the cyber armies of nation states rather than by other hackers.

Commercial purveyors of zero day malware have been known to charge over $1 million for a single exploit.

Poisoned Web Service Attacks

Many different types of attacks leverage vulnerabilities in servers, and new weaknesses are constantly discovered, which is why cybersecurity professionals have full-time jobs keeping servers safe. Entire books — or even several series of books — can be written on such a topic, which is, obviously, beyond the scope of this work.

That said, it is important for you to understand the basic concepts of server-based attacks because some such attacks can directly impact you.

One such form of attack is a *poisoned web service attack*, or a *poisoned web page attack*. In this type of attack, an attacker hacks into a web server and inserts code onto it that causes it to attack users when they access a page or set of pages that the server is serving.

For example, a hacker may compromise the web server serving `www.abc123.com` and modify the home page that is served to users accessing the site so that the home page contains malware.

But, a hacker does not even need to necessarily breach a system in order to poison web pages!

If a site that allows users to comment on posts isn't properly secured, for example, it may allow a user to add the text of various commands within a comment — commands that, if crafted properly, may be executed by users' browsers any time they load the page that displays the comment. A criminal can insert a command to run a script on the criminal's website, which can receive the authentication credentials of the user to the original site because it is called within the context of one of that site's web pages. Such an attack is known as *cross site scripting*, and it continues to be a problem even after over a decade of being addressed.

Network Infrastructure Poisoning

As with web servers, many different types of attacks leverage vulnerabilities in network infrastructure, and new weaknesses are constantly discovered. The vast majority of this topic is beyond the scope of this book. That said, as is the case with poisoned web servers, you need to understand the basic concepts of server-based attacks because some such attacks can directly impact you.

For example, criminals may exploit various weaknesses in order to add corrupt domain name system (DNS) data into a DNS server.

DNS is the directory of the Internet that translates human readable addresses into their numeric, computer-usable equivalents (IP

addresses). For example, if you type https://JosephSteinberg.com into your web browser, DNS directs your connection to an address of 104.18.45.53.

By inserting incorrect information into DNS tables, a criminal can cause a DNS server to return an incorrect IP address to a user's computer. Such an attack can easily result in a user's traffic being diverted to a computer of the attacker's choice instead of the user's intended destination. If the criminal sets up a phony bank site on the server to which traffic is being diverted, for example, and impersonates on that server a bank that the user was trying to reach, even a user who enters the bank URL into his or her browser (as opposed to just clicking on a link) may fall prey after being diverted to the bogus site. (This type of attack is known as *DNS poisoning* or *pharming*.)

Network infrastructure attacks take many forms. Some seek to route people to the wrong destinations. Others seek to capture data, while others seek to effectuate denial-of-service conditions. The main point to understand is that the piping of the Internet is quite complex was not initially designed with security in mind, and is vulnerable to many forms of misuse.

Malvertising

Malvertising is an abbreviation of the words malicious advertising and refers to the use of online advertising as a vehicle to spread malware or to launch some other form of a cyberattack.

Because many websites display ads that are served and managed by third-party networks and that contain links to various other third parties, online advertisements are a great vehicle for attackers. Even companies that adequately secure their websites may not take proper precautions to ensure that they do not deliver problematic advertisements created by, and managed by, someone else.

As such, malvertising sometimes allows criminals to insert their content into reputable and high-profile websites with large numbers of visitors (something that would be difficult for crooks to achieve otherwise),

many of whom may be security conscious and who would not have been exposed to the criminal's content had it been posted on a less reputable site.

Furthermore, because websites often earn money for their owners based on the number of people who click on various ads, website owners generally place ads on their sites in a manner that will attract users to the ads.

As such, malvertising allows criminals to reach large audiences via a trusted site without having to hack anything.

Some malvertising requires users to click on the ads in order to become infected with malware; others do not require any user participation — users' devices are infected the moment that the ad displays.

Drive-by downloads

Drive-by downloads is somewhat of a euphemism that refers to software that a user downloads without understanding what he or she is doing. A drive-by download may occur, for example, if a user downloads malware by going to a poisoned website that automatically sends the malware to the user's device when he or she opens the site.

Drive-by downloads also include cases in which a user knows that he or she is downloading software, but is not aware of the full consequences of doing so. For example, if a user is presented with a web page that says that a security vulnerability is present on his or her computer and that tells the user to click on a button that says Download to install a security patch, the user has provided authorization for the (malicious) download — but only because he or she was tricked into believing that the nature of the download was far different than it truly is.

Stealing passwords

Criminals can steal passwords many different ways. Two common methods include

- **Thefts of password databases:** If a criminal steals a password database from an online store, anyone whose password appears in

the database is at risk of having his or her password compromised. (If the store properly encrypted its passwords, it may take time for the criminal to perform what is known as a *hash attack,* but nonetheless, passwords — especially those that are likely to be tested early on — may still be at risk. To date, stealing passwords is the most common way that passwords are undermined.

- **Social engineering attacks:** *Social engineering attacks* are attacks in which a criminal tricks someone into doing something that he would not have done had he realized that the person making the request was tricking him in some way. One example of stealing a password via social engineering is when a criminal pretends to be a member of the tech support department of his target's employer and tells his target that the target must reset a particular password to a particular value to have the associated account tested as is needed after the recovery from some breach, and the target obeys. (For more information, see the earlier section on phishing.)
- **Credential attacks:** Credential attacks are attacks that seek to gain entry into a system by entering, without authorization, a valid username and password combination (or other authentication information as needed). These attacks fall into four primary categories:
    - *Brute force:* Criminals use automated tools that try all possible passwords until they hit the correct one.
    - *Dictionary attacks:* Criminals use automated tools to feed every word in the dictionary to a site until they hit the correct one.
    - *Calculated attacks:* Criminals leverage information about a target to guess his or her password. Criminals may, for example, try someone's mother's maiden name because they can easily garner it for many people by looking at the most common last names of their Facebook friends or from posts on social media. (A Facebook post of "Happy Mother's Day to my wonderful mother!" that includes a user tag to a woman

with a different last name than the user himself/herself is a good giveaway.)

- *Blended attacks:* Some attacks leverage a mix of the preceding techniques — for example, utilizing a list of common last names, or performing a brute force attack technology that dramatically improves its efficiency by leveraging knowledge about how users often form passwords.

- **Malware:** If crooks manage to get malware onto someone's device, it may capture passwords. (For more details, see the section on malware, earlier in this chapter.)
- **Network sniffing:** If someone transmits his or her password to a site without proper encryption while using a public Wi-Fi network, a criminal using the same network may be able to see that password in transit — as can potentially other criminals connected to networks along the path from the user to the site in question.
- **Credential stuffing:** In credential stuffing, someone attempts to log in to one site using usernames and passwords combinations stolen from another site.

REMEMBER You can utilize passwords and a password strategy that can help defeat all these techniques —see Chapter 7.

Exploiting Maintenance Difficulties

Maintaining computer systems is no trivial matter. Software vendors often release updates, many of which may impact other programs running on a machine. Yet, some patches are absolutely critical to be installed in a timely fashion because they fix bugs in software — bugs that may introduce exploitable security vulnerabilities. The conflict between security and following proper maintenance procedures is a never-ending battle — and security doesn't often win.

As a result, the vast majority of computers aren't kept up to date. Even people who do enable automatic updates on their devices may not be up to date — both because checks for updates are done periodically, not every second of every day, and because not all software offers automatic updating. Furthermore, sometimes updates to one piece of software introduce vulnerabilities into another piece of software running on the same device.

Advanced Attacks

If you listen to the news during a report of a major cyberbreach, you'll frequently hear commentators referring to advanced attacks. While some cyberattacks are clearly more complex than others and require greater technical prowess to launch, no specific, objective definition of an advanced attack exists. That said, from a subjective perspective, you may consider any attack that requires a significant investment in research and development to be successfully executed to be advanced. Of course, the definition of significant investment is also subjective. In some cases, R&D expenditures are so high and attacks are so sophisticated that there is near universal agreement that an attack was advanced. Some experts consider any zero-day attack to be advanced, but others disagree.

Advanced attacks may be opportunistic, targeted, or a combination of both.

Opportunistic attacks are attacks aimed at as many possible targets as possible in order to find some that are susceptible to the attack that was launched. The attacker doesn't have a list of predefined targets — his targets are effectively any and all reachable systems that are vulnerable to the attack that he is launching. These attacks are similar to someone firing a massive shotgun in an area with many targets in the hope that one or more pellets will hit a target that it can penetrate.

Targeted attacks are attacks that target a specific party and typically involve utilizing a series of attack techniques until one eventually succeeds in penetrating into the target. Additional attacks may be

launched subsequently in order to move around within the target's systems.

Opportunistic attacks

The goal of most opportunistic attacks is usually to make money — which is why the attackers don't care whose systems they breach; money is the same regardless of whose systems are breached in order to make it.

Furthermore, in many cases, opportunistic attackers may not care about hiding the fact that a breach occurred — especially after they've had time to monetize the breach, for example, by selling lists of passwords or credit card numbers that they stole.

While not all opportunistic attacks are advanced, some certainly are.

Opportunistic attacks are quite different than targeted attacks.

Targeted attacks

When it comes to targeted attacks, successfully breaching any systems not on the target list isn't considered even a minor success.

For example, if a Russian operative is assigned the mission to hack into the Democratic and Republican parties' email systems and steal copies of all the email on the parties' email servers, his or her mission is going to be deemed a success only if he achieves those exact aims. If he manages to steal $1 million from an online bank using the same hacking techniques that he is directing at his targets, it will not change a failure to breach the intended targets into even a small success. Likewise, if the goal of an attacker launching a targeted attack is to take down the website of a former employer that fired him, taking down other websites doesn't accomplish anything in the attacker's mind.

Because such attackers need to breach their targets no matter how well defended those parties may be, targeted attacks often utilize advanced attack methods — for example, exploiting vulnerabilities not known to the public or to the vendors who would need to fix them.

As you may surmise, advanced targeted attacks are typically carried out by parties with much greater technical prowess than those who carry out

opportunistic attacks. Often, but not always, the goal of targeted attacks is to steal data undetected or to inflict serious damage — not to make money. After all, if one's goal is to make money, why expend resources targeting a well-defended site? Take an opportunistic approach and go after the most poorly defended, relevant sites.

Some advanced threats that are used in targeted attacks are described as *advanced persistent threats* (APTs):

- **Advanced:** Uses advanced hacking techniques, likely with a major budget to support R&D
- **Persistent:** Keeps trying different techniques to breach a targeted system and won't move on to target some other system just because the initial target is well protected
- **Threat:** Has the potential to inflict serious damage

Blended (opportunistic and targeted) attacks

Another type of advanced attack is the opportunistic, semi-targeted attack.

If a criminal wants to steal credit card numbers, for example, he may not care whether he successfully steals an equivalent number of active numbers from Best Buy, Walmart, or Barnes & Noble. All that he or she likely cares about is obtaining credit card numbers — from whom the numbers are pilfered isn't relevant.

At the same time, launching attacks against sites that don't have credit card data is a waste of the attacker's time and resources.

Chapter 3

Bad Guys and Accidental Bad Guys: The Folks You Must Defend Against

IN THIS CHAPTER

- **Clarifying who the "good guys" are and who the "bad guys" are**
- **Understanding the different types of hackers**
- **Discovering how hackers make money from their crimes**
- **Exploring threats from nonmalicious actors**
- **Defending against hackers and other ways of mitigating against risks**

Many centuries ago, the Chinese military strategist and philosopher, Sun Tzu, wrote

> *If you know the enemy and know yourself, you need not fear the result of a hundred battles.*
>
> *If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.*
>
> *If you know neither the enemy nor yourself, you will succumb in every battle.*

As has been the case since ancient times, knowing your enemy is critical for your own defense.

Such wisdom remains true in the age of digital security. While Chapter 2 covers many of the threats posed by cyber-enemies, this chapter covers the enemies themselves:

- Who are they?
- Why do they launch attacks?
- How do they profit from attacks?

You also find out about nonmalicious attackers — both people and inanimate parties who can inflict serious damage even without any intent to do harm.

Bad Guys and Good Guys Are Relative Terms

Albert Einstein famously said that "Everything is relative," and that concept certainly holds true when it comes to understanding who the "good" guys and "bad" guys are online.

As someone seeking to defend himself or herself against cyberattacks, for example, you may view Russian hackers seeking to compromise your computer in order to use it to hack U.S. government sites as bad guys, but to patriotic Russian citizens, they may be heroes.

Likewise, if you live in the West, you may view the creators of *Stuxnet* — a piece of malware that destroyed Iranian centrifuges used for enriching uranium for potential use in nuclear weapons — as heroes. If you're a member of the Iranian military's cyber-defense team, however, your feelings are likely quite different. (For more on Stuxnet, see the nearby sidebar.)

STUXNET

Stuxnet is a computer worm that was first discovered in 2010 and is believed to have inflicted, at least temporarily, serious damage to Iran's nuclear program. To date, nobody has claimed responsibility for creating Stuxnet, but the general consensus in the information security industry is that it was built as a collaborative effort by American and Israeli cyberwarriors.

Stuxnet targets programmable logic controllers (PLCs) that manage the automated control of industrial machinery, including centrifuges used to separate heavier and

lighter atoms of radioactive elements. Stuxnet is believed to have compromised PLCs at an Iranian uranium-enrichment facility by programming centrifuges to spin out of control and effectively self-destruct, all while reporting that everything was functioning properly.

Stuxnet exploited four zero-day vulnerabilities that were unknown to the public and to the vendors involved at the time that Stuxnet was discovered. The worm was designed to propagate across networks — and spread like wildfire — but to go dormant if it didn't detect the relevant PLC and Siemens' software used at the Iranian facility.

If you're an American enjoying free speech online and make posts promoting atheism, Christianity, Buddhism, or Judaism and an Iranian hacker hacks your computer, you'll likely consider him to be a bad guy, but various members of the Iranian government and other fundamentalist Islamic groups may consider the hacker's actions to be a heroic attempt to stop the spread of blasphemous heresy.

In many cases, determining who is good and who is bad may be even more complicated and create deep divides between members of a single culture.

For example, how would you view someone who breaks the law and infringes on the free speech of neo-Nazis by launching a crippling cyberattack against a neo-Nazi website that preaches hate against African Americans, Jews, and gays? Or someone outside of law enforcement who illegally launches attacks against sites spreading child pornography, malware, or jihadist material that encourages people to kill Americans? Do you think that everyone you know would agree with you? Would U.S. courts agree?

Before answering, please consider that in the 1977 case *National Socialist Party of America v. Village of Skokie*, the U.S. Supreme Court ruled that freedom of speech goes so far as to allow Nazis brandishing swastikas to march freely in a neighborhood in which many survivors of the Nazi Holocaust lived. Clearly, in the world of cyber, only the eye of the beholder can measure good and bad.

For the purposes of this book, therefore, you need to define who the good and bad guys are, and, as such, you should assume that the language in the book operates from your perspective as you seek to

defend yourself digitally. Anyone seeking to harm your interests, for whatever reason, and regardless of what you perceive your interests to be, is, for the purposes of this book, bad.

Bad Guys Up to No Good

A group of potential attackers that is likely well-known to most people are the bad guys who are up to no good. This group consists of multiple types of attackers, with a diverse set of motivations and attack capabilities, who share one goal in common: They all seek to benefit themselves at the expense of others, including, potentially, you.

Bad guys up to no good include

- Script kiddies
- Kids who are not kiddies
- Nations and states
- Corporate spies
- Criminals
- Hacktivists

Script kiddies

The term *script kiddies* (sometimes shortened to skids or just kiddies) refers to people — often young — who hack, but who are able to do so only because they know how to utilize scripts and/or programs developed by others to attack computer systems. These folks lack the technological sophistication needed in order to create their own tools or to hack without the assistance of others.

Kids who are not kiddies

While script kiddies are technologically unsophisticated (see preceding section), plenty of other kids are not.

For many years, the caricature of a hacker has been a young, nerdy male, interested in computers, who hacks from his parents' home or from a

dorm room at college.

In fact, the first crop of hackers targeting civilian systems included many technologically sophisticated kids interested in exploring or carrying out various mischievous tasks for bragging rights or due to curiosity.

While such attackers still exist, the percentage of attacks emanating from these attackers has dropped dramatically from a huge portion to a minute fraction of a percentage of all attacks.

Simply put, teenage hackers similar to those depicted in movies from the 1980s and 1990s may have been a significant force in the precommercial-Internet-era, but once hacking could deliver real money, expensive goods, and valuable, monetizable data, criminals seeking to profit joined the fray en masse. Furthermore, as the world grew increasingly reliant on data and more government and industrial systems were connected to the Internet, nation and states began to dramatically increase the resources that they allocated to cyber-operations from both espionage and military standpoints, further diluting the classic teenage hacker to a minute portion of today's cyberattackers.

Nations and states

Hacking by nations and states has received significant press coverage in recent years. The alleged hackings of the Democratic party email systems by Russian agents during the 2016 Presidential election campaign and the Republican party email system during the 2018 midterm elections are high profiles examples of nation state hacking.

Likewise, the Stuxnet malware is an example of nation or state-sponsored malware. (For more on Stuxnet, see the sidebar earlier in this chapter.)

That said, most nation and state cyberattacks are not nearly as high profile as those examples, do not receive media coverage, and do not target high profile targets. Often, they're not even discovered or known to anyone but the attackers!

Furthermore, in some countries, it is difficult, if not impossible, to distinguish between nation or state hacking and commercial espionage.

Consider countries in which major companies are owned and operated by the government, for example. Are hackers from such companies nation or state hackers? Are such companies legitimate government targets, or is hacking them an example of corporate espionage?

Of course, nation and states that hack may also be seeking to impact public sentiment, policy decisions, and elections in other nations. Discussions of this topic have been aired via major media outlets on a regular basis since the 2016 presidential election.

Corporate spies

Unscrupulous companies sometimes utilize hacking as a way to gain competitive advantages or steal valuable intellectual property. The United States government, for example, has repetitively accused Chinese corporations of stealing the intellectual property of American businesses, costing Americans billions of dollars per year. Sometimes the process of stealing intellectual property involves hacking the home computers of employees at targeted companies with the hope that those employees will use their personal devices to connect to their employers' networks.

CHINESE FIRMS STEAL AMERICAN IP: UNIT 61398

In May 2014, United States federal prosecutors charged five members of the People's Liberation Army (PLA) of China with hacking four U.S. businesses and one labor union as part of their service in Unit 61398, China's cyber-warrior unit. The allegedly hacked parties included Alcoa, Allegheny Technologies, SolarWorld, and Westinghouse, all of which are major suppliers of goods to utilities, and the United Steel Workers labor union.

While the full extent of the damage to American businesses caused by the hacking remains unknown to this day, SolarWorld claimed that as a result of confidential information stolen by the hackers, a Chinese competitor appeared to have gained access to SolarWorld's proprietary technology for making solar cells more efficient. This particular case illustrates the blurred lines between nation and state and corporate espionage when it comes to Communist nations and also highlights the difficulty in bringing hackers who participate in such attacks to justice; none of the indicted parties were ever tried, because none have left China to any jurisdiction that would extradite them to the United States.

Criminals

Criminals have numerous reasons for launching various forms of cyberattacks:

- **Stealing money directly:** Attacking to gain access to someone's online banking account and issue a wire transfer of money to themselves.
- **Stealing credit card numbers, software, video, music files, and other goods:** Attacking to purchase goods or add bogus shipping instructions into a corporate system leading to products being shipped without payment ever being received by the shipper, and so on.
- **Stealing corporate and individual data:** Attacking to obtain information that criminals can monetize in multiple ways (see the section "Monetizing Their Actions," later in this chapter).

Over the years, the type of criminals who commit online crimes has evolved from being strictly solo actors to a mix of amateurs and organized crime.

Hacktivists

Hacktivists are activists who use hacking to spread the message of their "cause" and to deliver justice to parties whom they feel aren't being otherwise punished for infractions that the activists view as crimes. Hacktivists include terrorists and rogue insiders.

Terrorists

Terrorists may hack for various purposes, including to

- Directly inflict damage (for example, by hacking a utility and shutting off power)
- Obtain information to use in plotting terrorist attacks (for example, hacking to find out when weapons are being transported between facilities and can be stolen)
- Finance terrorist operations (see the earlier section on criminals)

Rogue insiders

Disgruntled employees, rogue contractors, and employees who have been financially incentivized by an unscrupulous party pose serious threats to businesses and their employees alike.

WARNING Insiders intent on stealing data or inflicting harm are normally considered to be the most dangerous group of cyberattackers. They typically know far more than do any outsiders about what data and computer systems a company possesses, where those systems are located, how they are protected, and other information pertinent to the target systems and their potential vulnerabilities. Rogue insiders may target a businesses for one or more reasons:

- They may seek to disrupt operations in order to lighten their own personal workloads or to help a competitor.
- They may seek revenge for not receiving a promotion or bonus.
- They may want to make another employee, or team of employees, look bad.
- They may want to cause their employer financial harm.
- They may plan on leaving and want to steal data that will be valuable in their next job or in their future endeavors.

Cyberattackers and Their Colored Hats

Cyberattackers are typically grouped based on their goals:

- **Black hat hackers** have evil intent and hack in order to steal, manipulate, and/or destroy. When the typical person thinks of a hacker, he or she is thinking of a black hat hacker.

- **White hat hackers** are ethical hackers who hack in order to test, repair, and enhance the security of systems and networks. These folks are typically computer security experts who specialize in penetration testing, and who are hired by businesses and governments to find vulnerabilities in their IT systems. A hacker is considered to be a white hat hacker only if he or she has explicit permission to hack from the owner of the systems that he or she is hacking.
- **Grey hat hackers** are hackers who do not have the malicious intent of black hat hackers, but who, at least at times, act unethically or otherwise violate anti-hacking laws. A hacker who attempts to find vulnerabilities in a system without the permission of the system's owner and who reports his or her findings to the owner without inflicting any damage to any systems that he or she scans is acting as a grey hat hacker. Grey hat hackers sometimes act as such to make money. For example, when they report vulnerabilities to system owners, they may offer to fix the problems if the owner pays them some consulting fees. Some of the hackers who many people consider to be black hat hackers are actually grey hats.
- **Green hat hackers** are novices who seek to become experts. Where a green hat falls within the white-grey-black spectrum may evolve over time, as does his or her level of experience.
- **Blue hat hackers** are paid to test software for exploitable bugs before the software is released into the market.

For the purposes of this book, black and gray hat hackers are the hackers that should primarily concern you as you seek to cyberprotect yourself and your loved ones.

Monetizing Their Actions

Many, but not all, cyberattackers seek to profit financially from their crimes. Cyberattackers can make money through cyberattacks in several ways:

- Direct financial fraud
- Indirect financial fraud
- Ransomware
- Cryptominers

Direct financial fraud

Hackers may seek to steal money directly through attacks. For example, hackers may install malware on people's computers to capture victims' online banking sessions and instruct the online banking server to send money to the criminals' accounts. Of course, criminals know that bank systems are often well-protected against such forms of fraud, so many have migrated to target less well-defended systems. For example, some criminals now focus more on capturing login credentials (usernames and passwords) to systems that store credits — for example, coffee shop apps that allow users to store prepaid card values — and steal the money effectively banked in such accounts by using it elsewhere in order to purchase goods and services. Furthermore, if criminals compromise accounts of users that have auto-refill capabilities configured, criminals can repetitively steal the value after each auto-reload. Likewise, criminals may seek to compromise people's frequent traveler accounts and transfer the points to other accounts, purchase goods, or obtain plane tickets and hotel rooms that they sell to other people for cash. Criminals can also steal credit card numbers and either use them or quickly sell them to other crooks who then use them to commit fraud.

REMEMBER *Direct* is not a black-and-white concept; there are many shades of grey.

Indirect financial fraud

Sophisticated cybercriminals often avoid cybercrimes that entail direct financial fraud because these schemes often deliver relatively small dollar amounts, can be undermined by the compromised parties even after the fact (for example, by reversing fraudulent transactions or

invalidating an order for goods made with stolen information), and create relatively significant risks of getting caught. Instead, they may seek to obtain data that they can monetize for indirect fraud. Several examples of such crimes include

- Profiting off illegal trading of securities
- Stealing credit card information
- Stealing goods
- Stealing data

Profiting off illegal trading of securities

Cybercriminals can make fortunes through illegal trading of securities, such as stocks, bonds, and options, in several ways:

- **Pump and dump:** Criminals hack a company and steal data, short the company's stock, and then leak the company's data online to cause the company's stock price to drop, at which point they buy the stock (to cover the short sale) at a lower price than they previously sold it.
- **Bogus press releases and social media posts:** Criminals either buy or sell a company's stock and then release a bogus press release or otherwise spread fake news about a company by hacking into the company's marketing systems or social media accounts and issuing false bad or good news via the company's official channels.
- **Insider information:** A criminal may seek to steal drafts of press releases from a public company's PR department in order to see whether any surprising quarterly earnings announcements will occur. If the crook finds that a company is going to announce much better numbers than expected by Wall Street, he or she may purchase *call options* (options that give the crook the right to purchase the stock of the company at a certain price), which can skyrocket in value after such an announcement. Likewise, if a company is about to announce some bad news, the crook may short the company's stock or purchase *put options* (options that give the crook the right to sell the

stock of the company at a certain price), which, for obvious reasons, can skyrocket in value if the market price of the associated stock drops.

Discussions of indirect financial fraud of the aforementioned types is not theoretical or the result of paranoid or conspiracy theories; criminals have already been caught engaging in precisely such behavior. These types of scams are often also less risky to criminals than directly stealing money, as it is difficult for regulators to detect such crimes as they happen, and it is nearly impossible for anyone to reverse any relevant transactions. For sophisticated cybercriminals, the lower risks of getting caught coupled with the relatively high chances of success translate into a potential gold mine.

AN INDIRECT FRAUD CASE THAT NETTED CYBERCRIMINALS MORE THAN $30 MILLION

During the summer of 2015, the United States Department of Justice announced that it filed charges against nine people — some in the United States and some in Ukraine — who it claimed stole 150,000 press releases from wire services and used the information in about 800 of those releases that had not yet been issued to the public to make illegal trades. The government claimed that the profits from the nine individuals' criminal insider trading activity exceeded $30,000,000.

Stealing credit card information

As often appears in news reports, many criminals seek to steal credit card numbers. Thieves can use these numbers to purchase goods or services without paying. Some criminals tend to purchase electronic gift cards, software serial numbers, or other semi-liquid or liquid assets that they then resell for cash to unsuspecting people, while others purchase actual hard goods and services that they may have delivered to locations such as empty houses, where they can easily pick up the items.

Other criminals don't use the credit cards that they steal. Instead, they sell the numbers on the dark web (that is, portions of the Internet that

can be accessed only when using technology that grants anonymity to those using it) to criminals who have the infrastructure to maximally exploit the credit cards quickly before people report fraud on the accounts and the cards are blocked.

Stealing goods

Besides the forms of theft of goods described in the preceding section, some criminals seek to find information about orders of high-value, small, liquid items, such as jewelry. In some cases, their goal is to steal the items when the items are delivered to the recipients rather than to create fraudulent transactions.

Stealing data

Some criminals steal data so they can use it to commit various financial crimes. Other criminals steal data to sell it to others or leak it to the public. Stolen data from a business, for example, may be extremely valuable to an unscrupulous competitor.

Ransomware

Ransomware is computer malware that prevents users from accessing their files until they pay a ransom to some criminal enterprise. This type of cyberattack alone has already netted criminals billions of dollars (yes, that is billions with a *b*) and endangered many lives as infected hospital computer systems became inaccessible to doctors. Ransomware remains a growing threat, with criminals constantly improving the technical capabilities and earning potential of their cyberweapons. Criminals are, for example, crafting ransomware that, in an effort to obtain larger returns on investment, infects a computer and attempts to search through connected networks and devices to find the most sensitive systems and data. Then, instead of kidnapping the data that it first encountered, the ransomware activates and prevents access to the most valuable information.

REMEMBER Criminals understand that the more important the information is to its owner, the greater the likelihood that a victim will be willing to pay a ransom, and the higher the maximum ransom that will be willingly paid is likely to be.

Ransomware is growing increasingly stealthy and often avoids detection by antivirus software. Furthermore, the criminals who use ransomware are often launching targeted attacks against parties that they know have the ability to pay decent ransoms. Criminals know, for example, that the average American is far more likely to pay $200 for a ransom than the average person living in China. Likewise, they often target environments in which going offline has serious consequences — a hospital, for example, can't afford to be without its patient records system for any significant period of time.

Cryptominers

A cryptominer, in the context of malware, refers to software that usurps some of an infected computer's resources in order to use them to perform the complex mathematical calculations needed to create new units of cryptocurrency. The currency that is created is transferred to the criminal operating the cryptominer. Many modern day cryptominer malware variants utilize groups of infected machines working in concert to do the mining.

Because cryptominers create money for criminals without the need for any involvement by their human victims, cybercriminals, especially those who lack the sophistication to launch high-stakes targeted ransomware attacks, have increasingly gravitated to cryptominers as a quick way to monetize cyberattacks.

While the value of cryptocurrencies fluctuates wildly (at least as of the time of the writing of this chapter), some relatively unsophisticated cryptocurrency mining networks are believed to net their operators more than $30,000 per month.

Dealing with Nonmalicious Threats

While some potential attackers are intent on benefiting at your expense, others have no intentions of inflicting harm. However, these parties can innocently inflict dangers that can be even greater than those posed by hostile actors.

Human error

Perhaps the greatest cybersecurity danger of all — whether for an individual, business, or government entity — is the possibility of human error. Nearly all major breaches covered in the media over the past decade were made possible, at least in part, because of some element of human error. In fact, human error is often necessary for the hostile actors to succeed with their attacks — a phenomenon about which they're well aware.

Humans: The Achilles' heel of cybersecurity

Why are humans so often the weak point in the cybersecurity chain — making the mistakes that enable massive breaches? The answer is quite simple.

Consider how much technology has advanced in recent years. Electronic devices that are ubiquitous today were the stuff of science-fiction books and movies just one or two generations ago. In many cases, technology has even surpassed predictions about the future — today's phones are much more powerful and convenient than Maxwell Smart's shoe-phone, and Dick Tracy's watch would not even be perceived as advanced enough to be a modern day toy when compared with devices that today cost under $100.

Security technology has also advanced dramatically over time. Every year multiple new products are launched, and many new, improved versions of existing technologies appear on the market. The intrusion detection technology of today, for example, is so much better than that of even one decade ago that even classifying them into the same category of product offering is questionable.

On the flip side, however, consider the human brain. It took tens of thousands of years for human brains to evolve from that of earlier species — no fundamental improvement takes place during a human lifetime, or even within centuries of generations coming and going. As such, security technology advances far more rapidly than the human mind.

Furthermore, advances in technology often translate into humans needing to interact with, and understand how to properly utilize a growing number of increasingly complex devices, systems, and software. Given human limitations, the chances of people making significant mistakes keep going up over time.

The increasing demand for brainpower that advancing technology places on people is observable even at a most basic level. How many passwords did your grandparents need to know when they were your age? How many did your parents need? How many do you need? And, how easily could remote hackers crack passwords and exploit them for gain in the era of your grandparents? Your parents? Yourself?

Most of your grandparents likely had no more than one or two passwords when they were your age — if not zero. And, none of these passwords were hackable by any remote computers — meaning that both selecting and remembering passwords was trivial, and did not expose them to risk. Today, however, you're likely to have many dozens of passwords, most of which can be hacked remotely using automated tools, dramatically increasing the relevant risk.

TIP The bottom line: You must internalize that human error poses a great risk to your cybersecurity — and act accordingly.

Social engineering

In the context of information security, *social engineering* refers to the psychological manipulation of human beings into performing actions that they otherwise would not perform and which are usually detrimental to their interests.

Examples of social engineering include

- Calling someone on the telephone and tricking that person into believing that the caller is a member of the IT department and requesting that the person reset his email password
- Sending phishing emails (see Chapter 2)
- Sending CEO fraud emails (see Chapter 2)

While the criminals launching social engineering attacks may be malicious in intent, the actual parties that create the vulnerability or inflict the damage typically do so without any intent to harm the target. In the first example, the user who resets his or her password believes that he or she is doing so to help the IT department repair email problems, not that he or she is allowing hackers into the mail system. Likewise, someone who falls prey to a phishing or CEO fraud scam is obviously not seeking to help the hacker who is attacking him or her.

Other forms of human error that undermine cybersecurity include people accidentally deleting information, accidentally misconfiguring systems, inadvertently infecting a computer with malware, mistakenly disabling security technologies, and other innocent errors that enable criminals to commit all sorts of mischievous acts.

WARNING The bottom line is never to underestimate both the inevitability of, and power of, human mistakes — including your own. You will make mistakes, and so will I — everyone does. So, on important matters, always double-check to make sure that everything is the way it should be.

External disasters

As described in Chapter 2, cybersecurity includes maintaining your data's confidentiality, integrity, and availability. One of the greatest risks to availability — which also creates secondhand risks to its

confidentiality and integrity — is external disasters. These disasters fall into two categories: naturally occurring and man-made.

Natural disasters

A large number of people live in areas prone to some degree to various forms of natural disasters. From hurricanes to tornados to floods to fires, nature can be brutal — and can corrupt, or even destroy, computers and the data that the machines house.

Continuity planning and disaster recovery are, therefore, taught as part of the certification process for cybersecurity professionals. The reality is that, statistically speaking, most people will encounter and experience at least one form of natural disaster at some point in their lives. As such, if you want to protect your systems and data, you must plan accordingly for such an eventuality.

A strategy of storing backups on hard drives at two different sites may be a poor strategy, for example, if both sites consist of basements located in homes within flood zones.

Man-made environmental problems

Of course, nature is not the only party creating external problems. Humans can cause floods and fires, and man-made disasters can sometimes be worse than those that occur naturally. Furthermore, power outages and power spikes, protests and riots, strikes, terrorist attacks, and Internet failures and telecom disruptions can also impact the availability of data and systems.

Businesses that backed up their data from systems located in New York's World Trade Center to systems in the nearby World Financial Center learned the hard way after 9/11 the importance of keeping backups outside the vicinity of the corresponding systems, as the World Financial Center remained inaccessible for quite some time after the World Trade Center was destroyed.

Risks posed by governments and businesses Some cybersecurity risks — including, one might reasonably argue, the most dangerous ones to individuals' privacy — are not created by criminals, but, rather, by businesses and government entities, even in Western democracies.

Cyberwarriors and cyberspies

Modern-day governments often have tremendous armies of cyberwarriors at their disposal.

Such teams often attempt to discover vulnerabilities in software products and systems to use them to attack and spy on adversaries, as well as to use as a law enforcement tool.

Doing so, however, creates risks for individuals and businesses. Instead of reporting vulnerabilities to the relevant vendors, various government agencies often seek to keep the vulnerabilities secret — meaning that they leave their citizens, enterprises, and other government entities vulnerable to attack by adversaries who may discover the same vulnerability.

Additionally, governments may use their teams of hackers to help fight crime — or, in some cases, abuse their cyber-resources to retain control over their citizens and preserve the ruling party's hold on power. Even in the United States, in the aftermath of 9/11, the government implemented various programs of mass data collection that impacted law-abiding U.S. citizens. If any of the databases that were assembled had been pilfered by foreign powers, U.S. citizens may have been put at risk of all sorts of cyberproblems.

The dangers of governments creating troves of data exploits are not theoretical. In recent years, several powerful cyberweapons believed to have been created by a U.S. government intelligence agency surfaced online, clearly having been stolen by someone whose interests were not aligned with those of the agency. To this day, it remains unclear whether those weapons were used against American interests by whoever stole them.

The impotent Fair Credit Reporting Act

Many Americans are familiar with the Fair Credit Reporting Act (FCRA), a set of laws initially passed nearly half a century ago and updated on multiple occasions. The FCRA regulates the collection and management of credit reports and the data used therein. The FCRA was

established to ensure that people are treated fairly, and that credit-related information remains both accurate and private.

According to the Fair Credit Reporting Act, credit reporting bureaus must remove various forms of adverse information from people's credit reports after specific time frames elapse. If you don't pay a credit card bill on time while you're in college, for example, it's against the law for the late payment to be listed on your report and factored against you into your credit score when you apply for a mortgage two decades later. The law even allows people who declare bankruptcy in order to start over to have records of their bankruptcy removed. After all, what good would starting over be if a bankruptcy forever prevented someone from having a clean slate?

Today, however, various technology companies undermine the protections of the FCRA. How hard is it for a bank's loan officer to find online databases of court filings related to bankruptcies by doing a simple Google search and then looking into such databases for information relevant to a prospective borrower? Or to see whether any foreclosure records from any time are associated with a name matching that of someone seeking a loan? Doing either takes just seconds, and no laws prohibit such databases from including records old enough to be gone from credit reports, and, at least in the United States, none prohibit Google from showing links to such databases when someone searches on the name of someone involved with such activities decades earlier.

Expunged records are no longer really expunged

The justice system has various laws that, in many cases, allow young people to keep minor offenses off of their permanent criminal records and affords judges the ability to seal certain files and to expunge other forms of information from people's records. These laws help people start over, and many wonderful, productive members of society may not have turned out as they did without these protections.

But what good are such laws if a prospective employer can find the supposedly purged information within seconds by doing a Google search on a candidate's name? Google returns results from local police blotters and court logs published in local newspapers that are now archived

online. Someone who was cited for a minor offense and then had all the charges against him or her dropped can still suffer professional and personal repercussions decades later — even though he or she was never indicted, tried, or found guilty of any offense.

Social Security numbers

A generation ago, it was common to use Social Security numbers as college ID numbers. The world was so different back then that for privacy reasons, many schools even posted people's grades using Social Security numbers rather than using students' names! Yes, seriously.

Should all students who went to college in the 1970s, 1980s, or early 1990s really have their Social Security numbers exposed to the public because college materials that were created in the pre-web world have now been archived online and are indexed in some search engines? To make matters worse, some parties authenticate users by asking for the last four digits of people's phone numbers, which can often be found in a fraction of a second via a cleverly crafted Google or Bing search. If it is common knowledge that such information has been rendered insecure by previously acceptable behaviors, why does the government still utilize Social Security numbers and treat them as if they were still private?

Likewise, online archives of church, synagogue, and other community newsletters often contain birth announcements listing not only the name of the baby and his or her parents, but the hospital in which the child was born, the date of birth, and the grandparents' names. How many security questions for a particular user of a computer system can be undermined by a crook finding just one such announcement? All of these examples show how advances in technology can undermine our privacy and cybersecurity — even legally undermining laws that have been established to protect us.

THE RIGHT TO BE FORGOTTEN

The *right to be forgotten* refers to the right of people to either have certain adverse data about them blocked from being Internet accessible or to have entries removed from search engine results on their names if the information in those entries is outdated or

irrelevant. Today, residents of the European Union enjoy the latter of these two rights; Americans enjoy neither.

The rationale behind the right to be forgotten is that it is clearly in society's interest that people not be forever negatively judged, stigmatized, and/or punished as a consequence of some long-ago minor infraction that doesn't represent the nature of their present self. For example, if a 45-year-old professional with a stellar professional and personal history and no criminal record applies for a job, it's unfair to him or her, and detrimental to society as a whole, if he or she would lose that opportunity because search engine results seen by a potential employer show that he or she was charged with disorderly conduct at age 18 for a nonviolent and non-damaging noisy prank carried out when he or she was an immature high school senior nearly three decades prior.

Various nations outside of the EU are also adopting various forms of the right to be forgotten: A court in India — a country that, technically speaking, has no laws on the books guaranteeing anyone the right to be forgotten — has ruled in favor of a plaintiff seeking the removal of accurate information that would reasonably have impacted her reputation, apparently adopting a position that people have an inherent right to prevent the spread of adverse information that may not be outdated, but that is likely to inflict harm on them while providing little benefit to anyone else.

Adopting some form of a right to be forgotten can help reduce some of the cybersecurity and privacy risks discussed in this chapter, by making it more difficult for criminals to obtain the answers to challenge questions, to launch social engineering attacks, and so on. It would also restore some of the protections offered by laws, such as the FCRA, that have been rendered impotent by technology.

Social media platforms

One group of technology businesses that generate serious risks to cybersecurity are social media platforms.

Cybercriminals increasingly scan social media — sometimes with automated tools — to find information that they can use against companies and their employees. Attackers then leverage the information that they find to craft all sorts of attacks, such as one involving the delivery of ransomware. (For more on ransomware, see the relevant section earlier in this chapter.) For example, they may craft highly effective spear-phishing emails credible enough to trick employees into clicking on URLs to ransomware-delivering websites or into opening ransomware-infected attachments.

The number of virtual kidnapping scams — in which criminals contact the family of a person who is off the grid due to being on a flight or the

like and demand a ransom in exchange for releasing the person they claim to have kidnapped — has skyrocketed in the era of social media, as criminals often can discern from looking at users' social media posts both when to act and whom to contact.

MOTHER'S MAIDEN NAME

How many times have you been asked your mother's maiden name as a security question in order to prove your identity?

Besides the fact that guessing any common English name will provide a criminal with some hits if he or she is attempting to impersonate people living in the United States, social media has truly undermined this form of challenge question. Cyberattackers can obtain this information from social media in many ways, even if people don't list their relatives in their profiles on any platform — for example, by trying the last names most commonly found among someone's Facebook friends. For many folks, one of those names will be their mother's maiden name.

Google's all-knowing computers

One of the ways that computer systems verify that a person is who he or she claims to be is by asking questions to which few people other than the legitimate party would know the correct answers. In many cases, someone who can successfully answer "How much is your current mortgage payment?" and "Who was your seventh grade science teacher?" is more likely to be the authentic party than an impersonator.

But the all-knowing Google engine undermines such authentication. Many pieces of information that were difficult to obtain quickly just a few year ago can now be obtained almost instantaneously via a Google search. In many cases, the answers to security questions used by various websites to help authenticate users are, for criminals, "just one click away."

While more advanced sites may consider the answer to security questions to be wrong if entered more than a few seconds after the question is posed, most sites impose no such restrictions — meaning that anyone who knows how to use Google can undermine many modern authentication systems.

Mobile device location tracking

Likewise, Google itself can correlate all sorts of data that it obtains from phones running Android or its Maps and Waze applications — which likely means from the majority of people in the Western World. Of course, the providers of other apps that run on millions of phones and that have permission to access location data can do the same as well. Any party that tracks where a person is and for how long he or she is there may have created a database that can be used for all sorts of nefarious purposes — including undermining knowledge-based authentication, facilitating social engineering attacks, undermining the confidentiality of secret projects, and so on. Even if the firm that creates the database has no malicious intent, rogue employees or hackers who gain access to, or steal, the database pose serious threats.

Such tracking also undermines privacy. Google knows, for example, who is regularly going into a chemotherapy facility, where people sleep (for most people, the time that they are asleep is the only time that their phones do not move at all for many hours), and various other information from which all sorts of sensitive extrapolations can be made.

Defending against These Attackers

REMEMBER It is important to understand that there is no such thing as 100 percent cybersecurity. Rather, adequate cybersecurity is defined by understanding what risks exist, which ones are adequately mitigated, and which ones persist.

Defenses that are adequate to shield against some risks and attackers are inadequate to protect against others. What may suffice for reasonably protecting a home computer, for example, may be wildly inadequate to shield an online banking server. The same is true of risks that are based on who uses a system: A cellphone used by the President of the United States for speaking with his or her advisors, for example, obviously

requires better security than the cellphone used by the average sixth grader.

Addressing Risks through Various Methods

Not all risks require attention, and not all risks that do require attention require addressing in the same manner. You may decide, for example, that buying insurance is sufficient protection against a particular risk or that the risk is so unlikely and/or de minimis so as to be not worth the likely cost of addressing it.

On the other hand, sometimes risks are so great that a person or business may decide to abandon a particular effort altogether in order to avoid the associated risk. For example, if the cost of adequately securing a small business would consistently be more than the profit that the business would have made without the security, it may be unwise to open up shop in the first place.