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 com-

puter 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; crimi-

nals 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 soft-

ware. 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, stigma-

tized, 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.