IN THIS CHAPTER

- Understanding 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

Chapter 1
What Exactly Is Cybersecurity?

To keep yourself and your loved ones cybersecure, you must first understand what cybersecure means. Along with that, you need to understand what your cybersecurity goals should be, and against what exactly you're securing yourself and your loved ones.

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

Cybersecurity Means Different Things to Different Folks

Although the word *cybersecurity* may sound like a simple enough word to define, in actuality, from a practical standpoint, it means quite different things to different people in different situations, leading to extremely varied policies, procedures,

and practices. Individuals who want to protect their social media accounts from hacker takeovers, for example, are unlikely to assume the approaches and technologies used by Pentagon workers to secure classified networks or CIA agents to protect the communications of spies.

Typically, for example:

- For **individuals,** *cybersecurity* means that their personal data is reliably accessible to them but not to anyone other than themselves and the others they have 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, that security cameras work properly and cannot be accessed by criminals, 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 housing 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 although the word cybersecurity is easy to define, the practical expectations that enter people's 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 these 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 terms. Technically speaking, for example, if someone writes down a password on a piece of paper and leaves the paper on a desk where other people can see the password instead of placing the paper in a safe deposit box or safe, that person has violated a principle of information security, not of cybersecurity, even though those actions may result in serious cybersecurity repercussions. Today, of course, paper documents can easily be scanned and thereby become

electronic records — so the lines between cybersecurity and information security have become quite blurry.

Cybersecurity Is a Constantly Moving Target

Although 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.

Although 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 areas and their impacts on the ever-evolving nature of cybersecurity: technological changes, and social, political, and economic model shifts.

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. Although 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

In the last few decades, we have witnessed dramatic changes in the technologies that exist, as well as in the people 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 only to people the owner recognized as authorized personnel and only when those people requested the key during business hours. For additional security, the data owner may have stored the cabinet in an office that was locked after business hours in a building that itself 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 steal people's images and leak them, hold them for ransom with ransomware, or use them to create turmoil in people's personal lives by creating fake profiles on dating sites, for example. 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, and, more specifically, the transformation of the Internet from a small network connecting researchers at a few universities to an enormous worldwide communication system utilized by a tremendous number of people, businesses, and organizations. In recent years, the Internet has also become the conduit for communication both by billions of smart devices and by people remotely connecting to industrial control systems. Just a few decades ago, it was unfathomable that hackers from across the globe could disrupt a business, manipulate an election, create a fuel shortage, pollute drinking water, 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. Cryptocurrency has dramatically magnified the potential return-on-investment for criminals involved in cybercrime, simultaneously increasing the crooks' ability to earn money through cybercrime and 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, and also allowed for the fast transfer of money across national borders without the need to use easily-traceable bank wires.

In addition, not only has the dramatic rise in the value of cryptocurrencies held by criminals over the past few years enriched many bad people, providing evildoers with the resources to invest in enhancing their cyber-arsenals, but also the public's perception of cryptocurrency as a quick way to get rich has helped scammers perpetuate all sorts of social engineering–based cybercrimes related to cryptocurrency investing.

Furthermore, the availability and global liquidity of cryptocurrency has helped criminals launder money obtained through the perpetration of all sorts of crimes. According to the U.S. government, cybercrime enabled by the existence of cryptocurrency has helped terrorists and drug traffickers finance their operations, and has even helped North Korea finance its nuclear program.

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. In later years, they may have connected to corporate networks via special dial-up connections using telephone-line–based private lines for extremely limited access to only one or two specific systems.

Connectivity to the Internet, of course, created risk, but initially most firewalls were set up in ways that did not allow people outside the organization to initiate communications — so, short of firewall misconfigurations 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.

Likewise, even in the relatively short time since the first edition of this book was published, the dramatic reduction in the cost of cellular-based high-speed Internet access and the availability of mobile data plans supporting speeds and data limits sufficient enough to allow effective full-time use have dramatically reduced the need for utilizing public Wi-Fi connections. Likewise, with the arrival of satellite-based Internet, humanity has grown closer to achieving its goal of true global Internet coverage. As such, public Wi-Fi-related risks that one might have deemed reasonable to take a few years ago in order to achieve various business aims have become unnecessary, and as such, policies and procedures regarding public Wi-Fi access must be updated, as is discussed later in this book in Chapters 7 and 21.

Smart devices

Likewise, the arrival of smart devices and the *Internet of Things* (the universe of devices that are connected to the Internet, but that are not traditional computers) — whose proliferation and expansion are presently occurring at a startling rate — means that unhackable solid-state machines such as classic washing machines and toaster ovens 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 18.

Globalization has also meant that cheap Internet of Things (IoT) devices can be ordered by consumers in one country from a supplier in another country halfway around the world — introducing without any oversight all sorts of unknown hardware into personal and corporate environments.

Even many types of medical equipment intended for consumer use have become "connected" — from CPAP machines to blood pressure measuring devices, thermometers, scales, and so on.

Artificial Intelligence

Artificial intelligence has had such a dramatic impact on cybersecurity, that an entire chapter about it has been added to this edition of the book.

Big data

Although 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, criminals can more easily than before identify ideal methods for social engineering their 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, and the practices of many organizations have invited all sorts of accusations around data misuse and inappropriate protections from both employees and outsiders. Additionally, the risks posed by Big Data are compounded when artificial intelligence is applied to them.

The COVID-19 pandemic

To many of us, the COVID-19 pandemic is an event we do not want to think about. But, although it was an awful time for humanity, it also served as a watershed moment in the history of cybersecurity. By forcing people to stay home in environments that are unprecedentedly isolated from one another, the novel coronavirus dramatically — and likely permanently — changed the way people in the Western world work, thereby yielding multiple, significant impacts on cybersecurity.

In the short term, the pandemic created all sorts of cybersecurity problems. Organizations that had no work-from-home infrastructures in place, or had such infrastructure but only for a limited portion of their employee populations, were suddenly faced with having to enable people to work from home — often without the ability to prepare users, policies, procedures, and technologies in advance. Many such businesses could not distribute laptops or security devices fast enough to prevent work stoppages, and as a result, relied on users to utilize their personal devices for work purposes without any additional security layers added.

Likewise, few organizations offered their employees separate Internet connections or separate routers for their remote workstations, so remote workers were nearly always sharing physical and logical networks with their other personal devices and possibly with their children who may have been gaming and/or attending virtual school. The security risks of doing such is discussed in detail in Chapter 6.

Compounding COVID-19–inflicted cybersecurity problems was the fact that although many employers provided some forms of endpoint security software, many did not, and even those that did rarely addressed any hardware-based risks. To this day, for example, many employers have no idea what router models their employees are using for remote access or when such devices were last updated.

Another major cybersecurity concern created by the pandemic has been that communications between employees shifted from conference rooms to remote

meetings, opening the doors for hackers to disrupt communications or steal confidential information. The problems were so bad that a new term *zoom bombing* was coined in 2020 to refer to the practice of mischievous folks joining and wreaking havoc in virtual meetings to which they were never invited.

Of course, the fact that people who would otherwise work together in the same location are suddenly unable to communicate quickly in person has also opened the door for many social engineering attacks. For example, a CFO who receives an email from the boss asking that the company pay a certain party for services can no longer verify the validity of the request by walking a few feet to confirm in person that the boss actually sent the message. Coupling the societal change with the deep fake capabilities provided by artificial intelligence has translated into a nightmare for some organizations.

Furthermore, people working in homes in which children are in virtual school, or quarantined, or simply living, often suffer from far more interruptions than they would had they been working in an office setting. Interruptions often lead to mistakes, and mistakes often lead to cybersecurity problems. The stress of remaining socially isolated for long periods of time also increases the odds of people making dangerous cybersecurity errors.

At a macro level, the sudden shift to work-at-home arrangements has meant that many cybersecurity professionals are increasingly overwhelmed, a problem further exacerbated by organizations having to reallocate resources — sometimes shifting both people and money from security projects to efforts to ensure continuity of operations.

And, of course, being confined to their homes has afforded many hackers more time to work on their crafts as well, perhaps contributing to the significant rise in the number of zero-day attacks and other newer forms of cybersecurity attacks seen since the pandemic's onset. Chapter 2 dives into many of the common cyberattacks that are out there.

REMEMBER

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. In addition, unforeseen developments, such as pandemics, can bring sudden, huge technological changes that carry with them tremendous cybersecurity dangers.

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 to dispel the perpetual propaganda the repressive countries use to explain their failure to produce a quality of life 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, or to provide misinformation to voters in the lands of their adversaries.

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. And the COVID-19 pandemic brought many of these issues to the forefront.

Furthermore, in many cases in which technological 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. No modern example portrays this as well as the sudden global shift to remote working arrangements in 2020.

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 the technologies a particular firm uses and for what purposes, or to discover people's travel schedules or 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, and unconcerned with, how much information about them lives on Internet-connected machines and how much other information about them can be extrapolated from the aforementioned data.

Likewise, just a few years ago, only a miniscule percentage of people had video cameras securing their homes. Thanks in part to Amazon's acquisition of Ring, the situation on the ground has changed dramatically — in some neighborhoods in which nobody had security cameras a decade ago, nearly every home today sports one or more Internet-connected cameras. Of course, while smart cameras located outside of one's home can create security and privacy issues, cameras

placed inside the home — as are becoming part of an increasingly common scenario — introduce all sorts of additional concerns.

All these changes have translated into a scary reality: Due to societal shifts, evil-doers can easily launch much larger, more sophisticated social engineering attacks today than they could just a few years ago. Coupling the social element with the technological advances makes the scary story even scarier.

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 an American company using a call center in India or a software development shop in the Philippines, have become the mainstay of many corporations. These changes, however, create cybersecurity risks of many kinds.

The last 25 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 entrepreneurs in New York seeking to have a logo made for their business could, shortly before going to bed, pay someone halfway around the globe $5.50 to create it and have the logo in their 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 more common than any locally sourced method of achieving similar results.

Of course, many cybersecurity ramifications result from such transformations of how people do business.

Data being transmitted needs to be protected from destruction, modification, and theft, and globalization means that greater assurance is needed to ensure 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. Code developed in foreign countries, for example, may be at risk of having backdoors inserted by agents of their respective governments. Likewise, computer equipment may have backdoors inserted into hardware components — a problem the U.S. government is struggling with addressing as this book goes to print. Additionally, when data travels through multiple areas, each involved jurisdiction's regulations related to security or privacy may apply.

WARNING

Hackers no longer necessarily need to directly breach the organizations they seek to hack; they merely need to compromise one or more of the organizations' product suppliers or service providers. And such third-parties may be less careful with their information security and personnel practices than the ultimate target, or may be subject to manipulation by governments far less respectful of people's rights than are the powers-that-be in the ultimate targets' location. Likewise, complex, multinational supply chains can lead to parties being unaware of who their providers actually are.

Political shifts

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

Sometimes, in the name of protecting their populations, government officials enact laws that do more harm than good. New Jersey's now-modified law that originally banned the sale of ordinary firearms as soon as smartgun technology became available led to a near-total cessation of research and development of guns that would fire only when the trigger was pulled by an authorized party; businesses won't invest in creating technologies that threaten to destroy the market for their flagship products. Today, various governments around the world are attempting to enact laws that protect children from adult content — but many of these laws place the impetus of age verification on the adult content providers, which means children remain exposed to online providers from every other jurisdiction, while government effectively delivers to parents a false sense of protection and discourages parents from taking better initiatives to protect their kids online. The effectiveness of the CHIPS Act — an effort to jumpstart the domestic development of technology hardware inside the USA to reduce our reliance on Communist China — was hampered (if not crippled) by the inappropriate inclusion in the act of socially oriented mandates that put conditions on the availability of grants to the few entities that could actually deliver on our national security needs. As will be discussed later, the threat of antitrust regulation against Microsoft may have even contributed to the major Crowdstrike-inflicted cyberattack of 2024.

Ordinary citizens need to understand the role politicians play in their cybersecurity — it is a mistake, for example, to rely on government promises of securing your children online overtaking action yourself. And, if you care about national security, you should hold elected officials responsible when they brag about delivering security through the implementation of new laws while those

laws prove impotent as a result of the politicians' actions, or when they act in fashions that cause technology companies to deliver unnecessarily vulnerable systems.

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 much easier access to a much greater amount of information about their potential intelligence targets than they could acquire even at dramatically higher costs just a few years ago. Coupled with the already low — and constantly dropping — cost of digital storage, advancing big-data technologies, artificial intelligence, and the expected eventual impotence of many of today's encryption technologies due to the emergence of quantum computing and other cutting-edge developments, governments have a strong incentive to collect and store as much information as they can about as many people as they can, in case it is of use at some later date. It is more likely than not, for example, that hostile governments may have already begun compiling dossiers on the people who will eventually serve as president and vice president of the United States 25 years from now.

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, for one nation to interfere 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 extremely risky.

In the not so distant past, in order for a government to spread misinformation and other propaganda, it had to print and physically distribute materials, or record and transmit messages via radio; misinformation campaigns were likely, therefore, 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 for doing so was relatively high, and often carried with it the potential for severe repercussions.

Manipulating voter registration databases to prevent legitimate voters from voting 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 nothing short of a traitor in order to have any real significant effect on election results. 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 reliably impact a major election would likely have been nearly impossible, and the odds of getting caught while attempting to do so were likely quite high.

Likewise, in the era of paper ballots cast in person and of manual vote counting, for a foreign power to manipulate actual vote counts on any large scale was impractical, if not 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 even rely on other people to help widely spread the misinformation — something that was impossible in the era of radio broadcasts, cassette 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 much-better funded parties could do in the past. Similarly, governments can spread misinformation to stir up civil discontent within adversarial nations and to spread hostility between ethnic and religious groups living in foreign lands.

Insecure mail-in ballots as used throughout the United States during the 2020 presidential election aggravated mistrust. And, 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 *is* 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, expressed at one point that that he believed 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, and even after a thorough FBI investigation into the matter. Statements and actions from the other side of the political aisle — including the terrible chaos at the U.S. Capitol after the 2020 presidential election — showed clearly that concerns about election integrity, and the perception that our elections might be manipulatable through cyberattacks and other technology-based techniques, are bipartisan.

Clearly, if online voting were ever to be adopted, 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.

In an indication of how much concern is growing around potential election manipulation, consider that until about 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.

Hacktivism

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. Likewise, citizens of one country may target entities in another country with whose policies they disagree, or whose government they consider a national adversary.

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 pertains to international sanctions: Rogue states subject to such sanctions have been able to use cybercrime of various forms to circumvent such 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. And, according to The White House, North Korea also commits all sorts of other cybercrimes to help fund its nuclear program.

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

New balances of power

Although 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.

Although 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 only trivially 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 can reasonably expect to 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 who 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 (for example, they claim, "we didn't do it, maybe someone else within our country did it" or the like), 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 10,000,001st attack launched against it, it may suffer a severe breach and make the news. Reports of the breach likely won't mention the fact that the company has a 99.999999 percent success rate in protecting itself 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, somehow neglected to fix a single vulnerability for which exploits already exist, it may suffer a severe breach. In such cases, media outlets will more likely than not point out the organization's failure to properly patch, with little mention of its near perfect record in that area.

As such, the era of cybercrime 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. Never mind that some cybercriminals around the globe may be agents of their local governments — or may have paid off local officials for "protection."

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 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, and in keeping humans safe from physical harm.

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 encompasses much more.

  Hackers that steal data undermine the data's 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 the data's 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 other professionals, leading to a "too many cooks in the kitchen" type challenge,

especially in larger organizations. A distributed denial-of-service attack is an example of an attempt to undermine availability. Also, consider that attackers often use tremendous numbers of hacked computers and their associated 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 and actually obtain legally.

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 portrays 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 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. Internet-connected cameras systems can also hold a treasure trove of private videos. 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. As noted above, such data can also sometimes be used to blackmail people.

- **Physical danger risks:** Cyberattacks on sewage treatment plants, utilities, and hospitals in recent years have shown clearly that the failure to maintain cybersecurity can lead to the endangering of human lives. For example, in 2020, it was reported that a woman in Germany died while being transported between hospitals after the hospital at which she had been a patient was struck by ransomware. And in 2021, a lawsuit was filed arguing that a baby died as a result of medical mistakes made as she was born at a hospital in Alabama during system outages caused by a ransomware attack.