Chapter 1

# What Exactly Is Cybersecurity?

IN THIS CHAPTER



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.



and protection schemes have been replaced with complex technologies that must automatically authenticate users who seek the data from po-

tentially 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 dol-

lars. 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 net-

works 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 op-

portunities 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 cyber-warriors 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 communica-

tion 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 fix-

tures 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 pro-

tect 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 quan-

tity 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-ser-

vice 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.