PART I

Cybersecurity Foundations

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

CHAPTER 1

Introduction to Cybersecurity

LEARNING OUTCOMES

By the end of this chapter, you will be able to:

- Discuss the history of cybercrime and cybersecurity.
- Identify key terms and key systems at risk.
- Differentiate between cybersecurity and other types of security.
- Describe the various types of threat actors and their motivations.
- Illustrate the need for risk management within cybersecurity and outline the factors that allow us to misperceive risk.

CHAPTER OUTLINE

Introduction

The old idiom that "crime doesn't pay" is not necessarily true for cybercrime. Globally, cybercrime costs trillions of dollars annually (Morgan, 2020), and only 10 percent of cybercrimes are actually reported to law enforcement in Canada (Schroeder, 2021).

Cybersecurity is no longer the sole responsibility of information technology (IT) professionals within an organization. It should be understood and weighed by the general population. The technical aspects of cybersecurity are important and need effective management, but the human and policy aspects are of equal importance and are often overlooked. Many cyberattacks occur as a result of human error—for example, a user not effectively locking down a system or clicking on a link that is intended to trick them. Human interaction increases risk. Increasingly, more of our data and interactions exist digitally. Many of us carry around at least one internet-connected device (e.g., a mobile phone) almost everywhere we go. If you have a health or fitness tracking watch, you are carrying around two. Maybe you have a third device, such as an insulin pump or a pacemaker. By 2030, it is projected that there will be at least 24 billion connected internet devices globally (CISOMAG, 2020)—that is 24 billion targets for cybercriminals. It makes sense that law enforcement has a difficult time keeping up.

Prior to 2020, not many people paid attention to cybersecurity. Companies typically placed cybersecurity responsibilities solely on IT. Cybersecurity training was not given to staff, nor was it included in briefings for executives. In 2019, the Canadian government reported that 21 percent of Canadian businesses were impacted by cybersecurity incidents—a percentage that continues to grow each year. Despite that statistic, just over half of those businesses (12 percent) reported the incident to police (Statistics Canada, 2020).

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

virtual private network (VPN)
a virtual network that is layered on top of an existing network designed to provide a secure communication mechanism for information transmitted over a public network such as the internet

Law enforcement, in many cases, is ill equipped to handle cybersecurity incidents. Attacks are often launched from outside the country and use special software such as **virtual private networks (VPNs)** to hide their location. In the case of extortion-style attacks, such as ransomware, computer files are locked by a virus and held hostage until the extortionist receives a cryptocurrency payment, which is virtually untraceable. Most companies turn to private firms to handle their cybersecurity incidents. More than half of the companies in Canada that are attacked by ransomware end up paying the ransom, according to a 2020 survey done by NOVIPRO (2020).

In early 2021, during the COVID-19 pandemic, approximately one third (32 percent) of Canadians worked from home (Mehdi & Morissette, 2021). This number went down as the pandemic ebbed; however, most of those employees continue to work from home part time. An increasing number of home networks are becoming a permanent extension of the corporate office network. This expands the responsibility of security managers from the equipment owned and managed by the company to all internet-connected devices/machines, including washing machines, thermostats, baby monitors, and more. Basically, anything that is connected to your home network may be a launch pad for attacks on you and the company you work for. Cybercrime from a law enforcement perspective and associated statistics will be covered in Chapter 2.

The internet was designed to be open and collaborative. It was not designed with security in mind. Fundamentally, the internet was built on the premise of information sharing. When you connect your laptop to the Wi-Fi at the local coffee shop, you are broadcasting all your data to every other computer that is connected to the same Wi-Fi. When the information leaves the coffee shop to travel to its destination, it goes through many computers (known as routers and switches), all owned by different organizations. For example, a simple test shows that data sent from one computer at Humber College Institute of Technology and Advanced Learning in Toronto to the University of British Columbia travels through more than 15 computers. All it takes is someone with a properly configured listening device along the way to record and decipher that information. These days, much of that information is encrypted, but encryption is not always foolproof. Encryption algorithms can be cracked—it just takes time to do so. A deeper dive on the internet and networking will be presented in Chapter 3.

The internet is evolving, and so are the threats. Encryption algorithms are advancing each year, but at some point in the near future, the current encryption paradigm will be broken by quantum computers. We will learn more about these evolving threats in Chapter 14.

Background

cybersecurity
the practice of protecting computer hardware, software, and digital information from unauthorized access or attacks

asset
anything that has value to the organization

What exactly is cybersecurity? While there are many different definitions, they all relate to the protection of technology and digital information. In this textbook, we will define **cybersecurity** as the practice of protecting computer hardware, software, and digital information from unauthorized access or attacks.

In other words, the protection of anything that is digitized or houses that digital information can be considered to be within the scope of cybersecurity practitioners. When we discuss protection, we need to clearly identify what we are protecting. In enterprises, we refer to those items as "assets." An **asset** is anything that has value to the organization (NIST, 2001).

The list of what an organization considers an asset varies. It could be people, equipment, software, accounts, and more. The RCMP, in their harmonized threat risk assessment methodology, has defined an extensive list of assets that serves as an excellent starting point for understanding what is typically defined as an organizational asset (RCMP, 2007). Assets will be discussed in more detail in the context of cybersecurity frameworks and cyber risk management in Chapters 8 and 11. Table 1.1 shows some examples of assets.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

TABLE 1.1 Examples of Assets

Physical	Digital
• Laptops • Desktops • Cellphones • USB and hard drives • IoT Devices • Networking Equipment	• Social media accounts • Online financial accounts • User accounts • Client information • Digital Medical Records • E-Signed or Scanned Contracts

There are some other types of security domains that overlap with cybersecurity. **Information security**, often referred to as InfoSec, is the practice of protecting information from unauthorized modification, disruption, destruction, or audit and deals with information in both digital and physical form. For example, a contract, a receipt, an employee record, or a design document could be in physical (paper) form or in a file on a computer.

information security the practice of protecting information from unauthorized modification, disruption, destruction, or audit

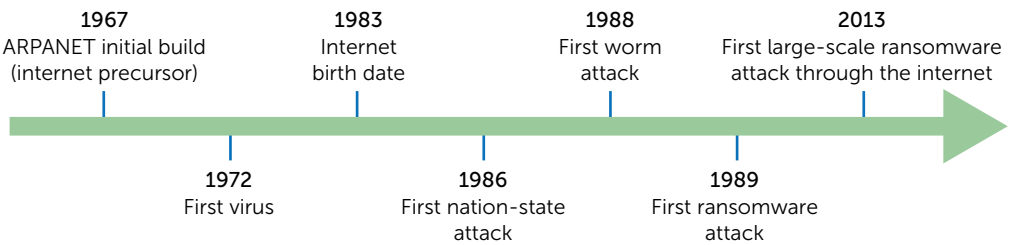
As you can see, there is a lot of overlap between information security and cybersecurity. In many organizations, the functions are merged into one team or the role of a single individual. Sometimes cybersecurity is the responsibility of the corporate security or IT departments. Other times, cybersecurity will have its own department that reports directly to the chief security officer or chief information security officer. We will discuss roles within security organizations in more detail in later chapters (Chapters 13 and 16). In this book, we will primarily focus on cybersecurity; however, concepts that overlap with information security and other roles will also be discussed.

A Brief History of Cybersecurity

ARPANET, the precursor to the internet, was built in 1967 (Andrews, 2013) and was fully operational by 1975. In 1971, four years prior, a computer scientist named Bob Thomas wrote Creeper, the first computer virus (Kaspersky, n.d.). The Creeper program was designed to copy itself from computer to computer, printing the message "I AM THE CREEPER; CATCH ME IF YOU CAN."

A timeline highlighting some key cybersecurity dates is included in Figure 1.1 and is explained below.

FIGURE 1.1 Timeline from ARPANET Launch to Key Attack Milestones



For most of the 1970s and early 1980s, cyberattacks were mainly from people inside an organization (insiders), such as employees or contractors reading and accessing unauthorized material.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

It was in 1983 that ARPANET adopted the communications protocol known as TCP/IP, which is still in use today. TCP/IP standardized communication between computers and between networks. It is this date, January 1, 1983, that is considered the birth date for the internet (Andrews, 2013). This milestone allowed people—including bad actors—to reach computers remotely and opened the door to many forms of cyberattack. Furthermore, TCP/IP and internet-based protocols make it difficult to determine with confidence the origin of the cyberattack—enabling those same bad actors to conduct their business with some degree of anonymity.

In 1986, Marcus Hess, a German citizen employed by the KGB, hacked into approximately 400 US government systems to find information about the Strategic Defense Initiative and other nuclear programs (Stoll, 1989). That information was then passed on to Russia. At the time, some large organizations, including the US military, connected remote computers by calling into a centrally located hub or gateway. Hess had access to the same gateway via a computer at a university in Germany. He realized that the communication links between the computers and the gateway were not very secure, and using this vulnerability, he was able to access the military computers unnoticed for an extended period of time. This attack, during the height of the Cold War (1947–1991), marks one of the first major cross-nation cyberattacks and the beginning of the Cyber War.

As we will learn later in the chapter, perpetrators of attacks have a wide range of motives. It was around the time of Marcus Hess when the personal computer revolution occurred, providing the average citizen with a device that they could use to write code (including viruses) and connect to the internet. In 1988, Robert Morris wanted to determine the size of ARPANET. His motives were simple curiosity and the desire to know whether it was possible. He created a type of computer virus, known as a worm, that copied itself and spread across the network. By definition, a **computer worm** is a type of malware that copies itself and spreads throughout the network without relying on other software programs (i.e., it is self-replicating). This caused a significant decrease in network speed, which caused Morris to be charged with a felony in the United States. He became the first person to be convicted under the US *Computer Fraud and Abuse Act*. Although his motives were not malicious, the consequences were. He didn't expect that his virus would have any negative impact on the network.

computer worm
a type of malware that copies itself and spreads throughout the network without relying on other software programs (i.e., it is self-replicating)

In 1990, a radio station in Los Angeles held a competition in which the 102nd caller (after a specific song was played) would win a Porsche 944 S2. Kevin Poulsen, a 24-year-old high school dropout, took control of the station's 25 phone lines, blocking out all calls but his own. Kevin was a new breed of cybercriminal, not focused on selling secrets to the highest bidder but rather building his own reputation as on online hacker. He was eventually caught and sentenced to five years in prison.

With the turn of the century, the scale of the attacks grew significantly. More people and businesses transitioned to online shopping. Companies began to store large amounts of their customers' personally identifiable information, including credit card information, on computers—with varying levels of susceptibility to cyberattacks. **Personally identifiable information (PII)** is information that can be used to clearly identify an individual. The information may be factual (such as a social insurance number) or subjective (such as opinions posted on social media). During this time, regulatory standards designed to manage this information were in the early stages, and governments had little oversight on how PII was managed or protected.

personally identifiable information (PII)
factual or subjective information that can be used to clearly identify an individual

In 2013, Target reported that hackers stole data of up to 40 million credit and debit cards of shoppers during the holiday season. This is one of the largest US retailer data breaches in history. Target was issued a fine of US$18.5 million as a result (Swinhoe, 2022). Hackers gained access to Target's point-of-sale (POS) system using credentials of a third-party contractor who had access to vulnerable systems (a huge oversight on Target's part). Hackers used that access to upload malware designed to skim customers' credit card credentials (PII) from the majority of Target's POS systems.

Over time, attacks have become more sophisticated and distributed and increasingly rely on anonymity. Tools have been made available that enable people to communicate in secret. While these tools help to protect people and their data, they are also readily used by threat actors.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

Threat actors are able to communicate with each other over the internet using tools that allow them to remain hidden from their victims and the authorities. A **threat actor**, also referred to as "bad actor," is an entity responsible for an incident that impacts or has the potential to impact the security of another entity.

threat actor
an entity responsible for an incident that impacts or has the potential to impact the security of another entity. These persons are also referred to as "bad actors".

The Internet and Types of Attacks

The internet can generally be divided into the public realm and the private realm. While we will learn more about computers and networking in Chapter 3, some basic concepts will be introduced here to better understand cybercrime and cybercriminals.

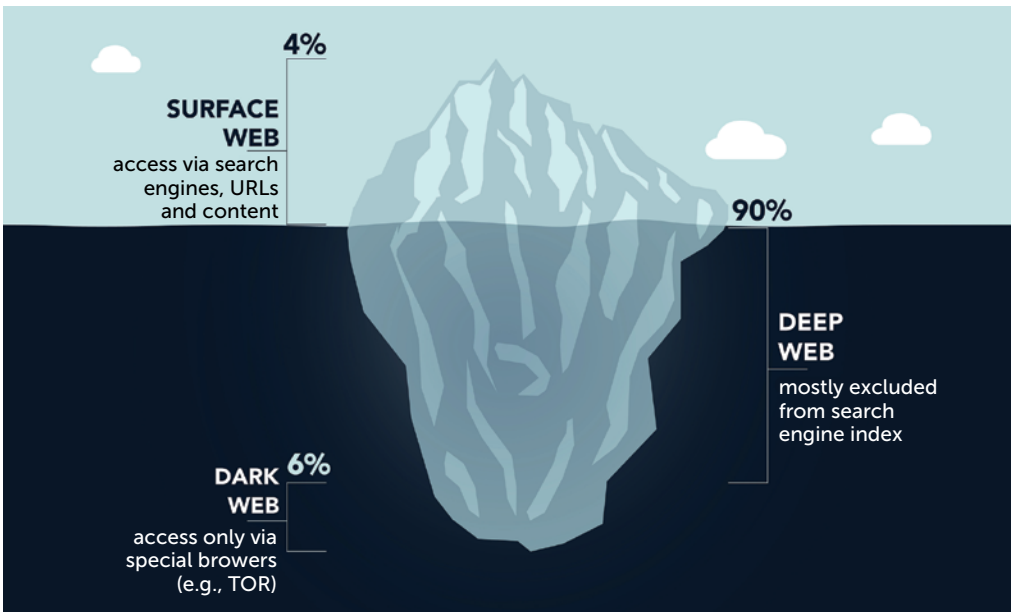
The public realm includes computers and servers (such as web servers and databases) that are easily accessed and are typically accessible by pre-installed web browsers on our computers or mobile devices. Furthermore, they do not require passwords to access. This part of the internet is often referred to as the clearnet or surface web. In other words, the **clearnet (surface web)** is the publicly addressable internet that typically includes websites and databases that can be easily accessed without specialized software or passwords. In addition, these locations are indexable by standard search engines. Examples of the clearnet include Facebook, Google, and YouTube.

clearnet (surface web)
the publicly addressable internet that typically includes websites and databases that can be easily accessed without specialized software or passwords and its locations are indexable by standard search engines

The internet is often thought about using the analogy of an iceberg (see Figure 1.2). The clearnet or surface web sits on top above the water while the rest of the internet (and the majority of it) sits beneath the water. This majority is referred to as the deep web or the invisible web (the private realm). The **deep web (invisible web)** is the part of the internet that cannot be accessed without specialized tools (e.g., software, hardware) or authentication (e.g., usernames, passwords). These locations are *not* indexable by standard search engines. Your online bank account is on the deep web. While you can easily reach your banking website via the clearnet, you cannot see your account details without entering your username and password (and possibly answering some additional security questions). Other deep web content includes personal social media accounts or online magazines or newspapers that require subscriptions before the content can be viewed (i.e., the content is behind a paywall).

deep web (invisible web)
the part of the internet that cannot be accessed without specialized tools (e.g., software, hardware) and/or authentication (e.g., usernames, passwords) and its locations are *not* indexable by standard search engines

FIGURE 1.2 Iceberg Analogy for the Surface Web, Deep Web, and Dark Web



This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

Most of the deep web is safe and used for legitimate and legal purposes. Anytime you connect to your work from home and connect to your office email, software, or databases, you are most likely using the deep web. There is a subset of the deep web that is designed to enhance or optimize user anonymity. This part is called the **dark web**. In order to access the dark web, you need specialized tools such as web browsers that do not come pre-installed on your computer. It is much more difficult for a user's activity to be surveilled when using these tools. The dark web is commonly used by dissidents and activists for planning activities and communicating with each other. In other cases, it is used to exchange information and hacking tools.

dark web
the part of the internet that runs on specialized networks; can only be accessed using specialized software and is designed to optimize user anonymity

Dark web communication is designed to be anonymous. Law enforcement is continually finding ways to monitor this communication, but it is near impossible for local law enforcement. This anonymity enables clandestine interactions.

On March 20, 2000, Freenet, the first anonymity-focused network, was launched. A few years later, another anonymity-based network known as Tor was released. The Tor network has grown to be the largest anonymity network in the world (and is used for both legal and illegal purposes). Not long after the launch of these networks, the dark web surfaced, and with it one of the first and most popular online black markets called Silk Road. The website was launched in February 2011 by its founder, Ross Ulbricht. Silk Road was operational for two years. According to *The Guardian* news outlet, is estimated that it had had over 100,000 buyers and over 10,000 products for sale. Approximately 70 percent of the items for sale were drugs (Olson, 2013). The website also sold illegal services, weapons, credit cards, identifications, and so on. In 2013, the FBI arrested Ulbricht and shut down the website. Ulbricht was eventually sentenced to life in prison without the possibility of parole. Since that time, many other dark marketplaces and illegal websites have surfaced on the dark web. Law enforcement works to take them down each time, although the process is cumbersome and long as the founders and sites are often located in countries that are unwilling or unable to cooperate in these investigations (due, in part, to resource availability or expertise).

The primary form of currency exchanged in these clandestine encounters and online marketplaces is cryptocurrency. **Cryptocurrency** is a digital currency that exists only electronically and is not regulated by any one country or financial institution—making it difficult to trace. Transactions are managed and records maintained by a decentralized set of computers that are typically distributed across the internet. There are many different cryptocurrency brands. Cryptocurrency technology will be discussed in more detail in later chapters.

cryptocurrency
digital currency that exists only electronically and is not regulated by any one country or financial institution, making it difficult to trace

Through leveraging both the dark web and cryptocurrencies, bad actors are now able to launch attacks that are very difficult to trace. One of the most popular forms of attack are ransomware attacks. Bad actors typically launch ransomware attacks via email from the dark web and then subsequently hold a victim's data or systems hostage until they receive payment anonymously via cryptocurrency. The first documented ransomware attack was not actually distributed through the internet but rather through floppy disks. It was developed by Joseph Popp, an AIDS researcher, and was known as the AIDS Trojan or PC Cyborg. In 1989, Popp mailed 20,000 floppy disks to AIDS researchers globally. The floppy disks contained malware that was activated once the computer was turned on 90 times. Once the threshold was reached, the files would be encrypted and a message would appear on the screen directing the victims to mail $189 to a post office box in Panama. These days, ransomware is distributed through the internet.

In September 2013, most of the world first heard the term "ransomware" when an early form of ransomware known as CryptoLocker crippled more than 250,000 computer systems globally (Kelion, 2013). Victims were told to pay the ransom using cryptocurrency or money cards—delivering an estimated millions of dollars to the attackers (Olson, 2014). When users of infected computers booted up their computer, they would see the image in Figure 1.3.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

FIGURE 1.3 CryptoLocker Ransomware Message from 2013 Attack

Today, we have many types of attacks. We have attacks such as ransomware that come from the dark web over email. We have attacks through third-party software or through suppliers connecting to a company's network. We have attacks that occur through people accidently disclosing confidential information. Other attacks come in through existing vulnerabilities or misconfigurations in our systems.

Cyberattacks first require the attacker to install specialized software tools on their computer. These tools provide the framework for launching the attack. Many of these tools are available for free on the internet and come prepackaged in various operating systems, such as Kali Linux, Parrot OS, and Blackbox, among others. They are typically free and legal in most jurisdictions. Often these tools are used by ethical hackers and security personnel as part of their approved security testing activities. Using these tools to launch cyberattacks is illegal. For some attacks, such as ransomware, attackers will license or purchase other tools via the dark web (which may or may not be legal). A successful attack most often requires additional software tools to be installed on the target computer without the knowledge or authorization of the owner or operator of that

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

malware
software installed on a computer with the potential to harm or exploit the same or another computer or system

computer. The software that is installed on the target computer is referred to as **malware**, which is software installed on a computer with the potential to harm or exploit the same or another computer (or system).

This book will explore the various ways malware can be deployed, including via email, USB thumb drives, fake websites, zero-day flaws and bugs, and more. Each of these will be defined and discussed thoroughly in this text.

Who Are the Attackers?

As soon as new technology is launched, there will be individuals who will try to break, reverse engineer, or infiltrate that technology. It may be a whole new platform, a new app, a new smart home device, or a software upgrade. In many cases, the intent is not criminal in nature, and those individuals are doing it for fun, fame, or financial gain. There are many blogs and sites that pay individuals for that information. That information can, in turn, be used by certain people to infiltrate computers and networks for various purposes. Collectively we refer to these individuals as threat actors. As mentioned earlier, a threat actor (or bad actor) is an entity responsible for an incident that impacts or has the potential to impact the security of another entity.

STUXNET

Stuxnet was a computer worm that, when injected into a computer network, seeks out specific types of industrial computers used to control various devices such as centrifuges. An attack was reportedly launched on 14 Iranian industrial sites, including at least one facility that enriched uranium, destroying the centrifuges. The attack was nation-state sponsored, and leaks to the press strongly suggest that both the United States and Israel were behind the attack.

The computer worm leveraged what is called a zero-day flaw in the Windows operating system. Discussed in more detail later, these zero-day flaws are unknown or undetected vulnerabilities in a system. Bad actors will exploit these vulnerabilities to gain access to the target systems.

Stuxnet was detected in 2010 but is thought to have been in development since 2005. It took years to develop both the malware and to plan the attack. The malware was introduced by simply inserting an infected USB into a computer on the target network.

What exactly is the motivation of these threat actors? It depends. Sometimes it is politically motivated. Sometimes it is financially motivated. Capability and sophistication of the threat actors varies widely as well. The threat actors are typically segmented into the following categories:

- *Nation-state actors.* Funded by governments, these groups are both highly sophisticated and highly capable. The objective is to inflict damage or harm to other governments or nations. Their attacks are often planned years in advance. One of the earliest and best-known attacks was Stuxnet (Kushner, 2013). In most cases, nation-states will employ the services of private companies to identify their target's technical vulnerabilities, tools that can be used in the attack, or resources who are responsible for carrying out the attack. This model helps to shield the nation-states from identification if the attack is traced back to its source.
- *Insider threats.* These are individuals working within the target organization. They may be disgruntled employees, subcontractors, or consultants who are not happy with their current working situation. It may be individuals who simply make mistakes or are tricked into unauthorized disclosure of information. These individuals do not necessarily have sophisticated skills. They often have access to restricted, employee-only systems (via usernames and passwords). Each year, the media reports many examples of these types of attacks. In one such case in September 2017, Coca-Cola announced an attack where a former em-

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

ployee took a hard drive containing the PII of approximately 8,000 workers, including their names, social security numbers, addresses, ethnicity, credit card data, financial data, and other data (Cyware Hacker News , 2018). That theft didn't require advanced skills; however, the data could be used to commit identity theft and various financial frauds.

- *Organized cybercriminals.* While these threat actors are also well funded and sophisticated (similar to nation-state actors), the objective of organized cybercriminals is primarily financial gain or influence. The model employed by these organizations is often multilayered and similar to that of the drug trade. Often the front-line criminals (who are less sophisticated) will deploy an attack via email. Once the user clicks on the email, the malware installs and communicates back to the more sophisticated "behind the scenes" threat actors who manage the attack or negotiations with the victim from deep in the dark web. The front-line threat actors typically have some sort of profit-sharing arrangement with the hidden dark web actors (who are often anonymous). When law enforcement investigates, it is often the front-line threat actors who are caught while the dark web actors remain hidden and anonymous. Payment is typically made in cryptocurrency, making it difficult to trace.
- *Hacktivists and terrorist groups.* The motivation for both these groups is similar in that both want to create change. Hacktivists seek ideological change, whereas terrorist groups tend to seek political change. Both groups tend to have relatively low levels of sophistication and capability and often rely on technical tools that can be easily obtained and do not require a significant investment in technical development. In 2010, a hacktivist group named Anonymous carried out an attack on an underground pedophile community known as Lolita City, which was a child pornography hosting site on the dark web. In their multilayered attack, they first started by flooding the web servers with information. This attack, known as a DDoS (distributed denial of service) attack, will be discussed later in the book. It had the effect of making the website inaccessible in its entirety. Eventually they published the names of the 1,589 users of the site, inviting Interpol and the FBI to investigate further.
- *Thrill seekers or script kiddies.* These groups are typically in the business of building a reputation online. Often these individuals are using scripts or programs they downloaded from the internet to conduct relatively simple types of attacks (such as password cracking).

A summary of the characteristics of these threat actors is provided in Table 1.2.

TABLE 1.2 Characteristics of Threat Actors

Cyber Threat Actor	Motivation	Sophistication		Capability		Access to Target Materials		Resources	
		High	Low	High	Low	Easy	Difficult	Few	Many
Nation-state	Geopolitical influence	✔		✔			✔		✔
Insider threat	Unhappiness		✔		✔	✔		✔	
Organized cybercriminal	Financial gain	✔		✔			✔		✔
Hacktivist	Ideological		✔		✔		✔	✔	
Terrorist	Political		✔		✔		✔	✔	
Thrill seekers/ script kiddies	Reputation		✔		✔		✔	✔	

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

Managing Cybersecurity Risk

Cyber risk management will be discussed in detail in Chapter 11. However, it is important, at this point, to discuss some of the basics as there are common terms and ideas related to risk that are used throughout the practice of cybersecurity.

Let's start with the term "risk." We experience risk in every part of lives each and every day. Risk is unavoidable. Risk, simply stated, is the chance that an outcome will happen. That could be the chance of getting seriously injured while jaywalking across a street or the chance of winning $1 million in the lottery. While we are all innately programmed to perceive risk, we do not necessarily judge the severity of that risk accurately. How we perceive risks, misperceive risks, or tolerate them is a whole field of study within psychology. Our perception of that severity is based on a variety of factors that are beyond the scope of this book, some of which are identified in Figure 1.4.

FIGURE 1.4 Perception of Risk Severity

Positive Versus Negative Impact

Our perception of the benefit of an activity may make us less worried about the negative consequences (e.g., bungee jumping) (Block & Keller, 1995)

Awareness and Media Coverage

Our perception of the risk is impacted by the information provided to us through traditional and social media (e.g., the risks associated with vaccines may be perceived differently by people depending on the content in their social feeds) (McCarthy et al., 2008)

The Dread Factor

We tend to perceive risks with painful or traumatic consequences as more severe than they actually are due to their low likelihood (e.g., being eaten by a shark) (Slovic, 2000)

Acute Versus Chronic

We tend to be more fearful of events that can impact many of us at once than we are of events that impact us over time (e.g., a plane crash versus pollution) (Slovic, 2000)

Implicit Bias

Our cultural roots and lived experiences impact how we interpret and perceive events and people. Our automatic inclination to assign particular attributes or qualities to people or situations is known as "implicit bias." Implicit bias leads to misperceiving how likely a risk is to occur (e.g., the fact that an employee has never been a victim of an attack may make them think they do not need to attend a cybersecurity training session) (Staats, 2012)

When you layer on the fact that one of the biggest security threats facing any organization (especially cybersecurity) is its people, we see how critical it is to minimize misperceptions of risk. People are making decisions about which email links to click on, which passwords to change, how networks are to be configured, whether or not suppliers are given access, and much more. If people are misperceiving the risk level when making these decisions, they are unnecessarily exposing the organization.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

In fact, most data breaches and attacks can be traced back to a person within the organization. That person has typically been tricked or "socially engineered" to divulge or give access to restricted information or systems to someone they should not—someone who is unauthorized. **Social engineering** is the art of manipulating someone to divulge or give access to restricted information or systems. This in turn can then be used to commit illegal activities, such as fraud and theft. It may be as simple as an employee posting seemingly harmless personal and work-related information on social media. Hackers might use this publicly available information in phishing emails to gain access to enterprise systems via an employee's computer, ultimately resulting in detrimental security breaches. These types of attacks will be discussed in later chapters.

social engineering
the art of manipulating someone to divulge or give access to restricted information or systems

Organizations should take a systematic approach to managing risk to ensure that unbiased, evidence-based decisions are made. To facilitate that, many organizations implement a methodology to define and assess risk and the associated terminology. We use the definition of risk from the International Standards Organization: **risk** is the effect of uncertainty on the objectives (ISO, 2018).

risk
the effect of uncertainty on an organization's objectives (ISO, 2018), or simply the chance that an outcome will happen

Within an enterprise, uncertainty can refer to everything from a flood causing damage to key infrastructure to a customer posting a negative review on social media to a specific type of cyberattack. We will focus on uncertainties related to cybersecurity.

Objectives, from an organizational perspective, may be general (e.g., maintaining business continuity or make a profit) or specific (e.g., restricting access to sensitive customer data or protect trade secrets). Those objectives are typically achieved through normal business operations. Cyber threats may adversely impact the organization's ability to achieve their objectives. A **cyber threat** is any circumstance, situation, or event with the potential to adversely impact business operations, organizational assets, or individuals.

cyber threat
any circumstance, situation, or event with the potential to adversely impact business operations, organizational assets, or individuals

Once the organization identifies the risks and prioritizes them accordingly, they are systematically able to address them (ensuring that the time, budget, and resources allocated to this endeavour are used to address the highest priority threats first).

Many organizations have robust operations and are able to withstand many types of cyberattacks. Others are not able to prevent even basic infiltration. Quantifying this level of vulnerability allows the organization to more effectively measure the uncertainty associated with the threat of attack.

A threat actor needs something to exploit to gain entry into an organization. In some cases, that exploitation may involve convincing an employee to give them access to a system or information. In other cases, it may be through a pre-existing vulnerability on a specific computer. These exploitation points are referred to as the cyber threat surface. **Cyber threat surfaces** are all computer endpoints that connect the organizational assets to the internet. These endpoints may be connected directly to the internet via technology (e.g., internet-connected storage or systems) or may be connected through a person (e.g., a person divulging PII to an unauthorized individual on the internet).

cyber threat surface
all computer endpoints that connect the organization's assets to the internet

Those endpoints may be both physical and in software. Examples of these connections include laptops, smartphones, alarm systems, databases, credit card terminals, and more. Sometimes these are onsite, and sometimes they are in the cloud. They may even be at an employee's home if they are permitted to work remotely. Services, devices, and data can all be targeted to compromise business operations (e.g., supply chain systems). As the number of devices continues to expand, so does the threat surface (and the possible points of entry). These threats are carried out by cyber threat actors (described earlier in the chapter).

There are lots of strategies for measuring and managing risk within organizations. Those will be discussed later in the book.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

What to Expect from This Book

By the end of this book, the reader should have a solid foundation in cybersecurity from a terminology, a technology, an operational, and a policy perspective. This book is broad and covers many aspects of cybersecurity. It is organized into four broad categories:

- *Part 1: Cybersecurity Foundations.* The first two chapters focus on introducing the reader to the general area of cybersecurity, its history, and its criminal landscape within Canada. Chapter 3 provides an overview of computers, networks, and internet architecture.
- *Part 2: Unmasking Cybersecurity.* The next four chapters (Chapters 4–7) delve deep into the attack landscape and associated vulnerabilities and controls.
- *Part 3: Cybersecurity Operations.* Chapters 8–12 present the reader with the tools and techniques for managing cybersecurity within the enterprise.
- *Part 4: Other Considerations and Conclusions.* The last two chapters (Chapters 13 and 14) invite the reader to step back and think about where cybersecurity is headed and how to holistically protect the enterprise.

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

REVIEW QUESTIONS

1. What is the difference between information security and cybersecurity? Give one example of each (that is not within the scope of the other).
2. Explain why you cannot access the dark web with a regular web browser.
3. Name five endpoints in the workplace and five endpoints in your home that could be considered part of the cyber threat surface.

KEY TERMS

asset, 4
clearnet (surface web), 7
computer worm, 6
cryptocurrency, 8
cybersecurity, 4
cyber threat, 13
cyber threat surface, 13
dark web, 8
deep web (invisible web), 7
information security, 5
malware, 10
personally identifiable information (PII), 6
risk, 13
social engineering, 13
threat actor, 7
virtual private network (VPN), 4

REFERENCES

Andrews, E. (2013, December 18). *Who invented the internet?* History.com. https://www.history.com/news/who-invented-the-internet

Block, L.G., & Keller, P.A. (1995). When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform a health-related behavior. *Journal of Marketing Research*, *32*(2), 192–203.

CISOMAG. (2020, May 29). *Number of IoT devices expected to reach 24.1 bn in 2030: Report*. CISO Mag. https://cisomag.com/number-of-iot-devices-expected-to-reach-24-1-bn-in-2030-report/

Computer Fraud and Abuse Act, 18 USC § 1030.

Cyware Hacker News. (2018, May 28). *Coca-Cola suffers breach after ex-employee steals hard drive with 8000 workers' data*. Cyware. https://cyware.com/news/coca-cola-suffers-breach-after-ex-employee-steals-hard-drive-with-8000-workers-data-59747f8c

ISO. (2018). *ISO 31000:2018*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Kaspersky. (n.d.). *A brief history of computer viruses & what the future holds*. https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds

Kelion, L. (2013, December 24). *CryptoLocker ransomware has "infected about 250,000 PCs."* BBC News. https://www.bbc.com/news/technology-25506020

Kushner, D. (2013, February 26). *The real story of Stuxnet*. IEEE Spectrum. https://spectrum.ieee.org/the-real-story-of-stuxnet

McCarthy, M., Brennan, M., De Boer, M., & Ritson, C. (2008). Media risk communication—what was said by whom and how was it interpreted. *Journal of Risk Research, 11*(3), 375–394. DOI: 10.1080/13669870701566599

Mehdi, T., & Morissette, R. (2021, April 1). Working from home: Productivity and preferences. Statistics Canada Catalogue no. 45280001. https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00012-eng.htm

Morgan, D. (2020, November 9). *Global cybercrime damages predicted to reach $6 trillion annually by 2021*. Cybercrime Magazine. https://cybersecurityventures.com/annual-cybercrime-report-2020

NIST. (2001, June). *NISTIR 7693, Specification for Asset Identification 1.1*. Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7693.pdf

NOVIPRO. (2020, January 27). *2020 IT portrait of Canadian medium and large sized companies*. https://hub.novipro.com/en/2020-it-portrait

Olson, P. (2013, November 10). *The man behind Silk Road—the internet's biggest market for illegal drugs*. The Guardian. https://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.

Olson, P. (2014, February 3). *CryptoLocker thieves likely making "millions" as Bitcoin breaks $1,000*. Forbes. https://www.forbes.com/sites/parmyolson/2013/11/27/cryptolocker-thieves-likely-making-millions-as-bitcoin-breaks-1000/?sh=7e97f9b67535

RCMP. (2007, October 23). *RCMP publications.* https://cyber.gc.ca/sites/default/files/publications/tra-emr-1-e.pdf

Schroeder, B. (2021, December 22). *Policing cybercrime*. Blue Line. https://www.blueline.ca/policing-cybercrime

Slovic, P. (2000). Perception of risk. In P. Slovic (Ed.), *The perception of risk* (pp. 220–231). Earthscan.

Staats, C. (2012, April 12). *Implicit bias and (mis)perceptions*. Kirwan Institute for the Study of Race and Ethnicity. https://kirwaninstitute.osu.edu/article/implicit-bias-and-misperceptions

Statistics Canada. (2020, October 20). About one-fifth of Canadian businesses were impacted by cyber security incidents in 2019. *The Daily*. Catalogue no. 11-001-X. https://www150.statcan.gc.ca/n1/daily-quotidien/201020/dq201020a-eng.htm

Stoll, C. (1989). *The cuckoo's egg: Tracking a spy through the maze of computer espionage.* Gallery Books.

Swinhoe, D. (2022, January 28). *The biggest data breach fines, penalties, and settlements so far*. CSO Online. https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

This excerpt is for review purposes only, and may not be shared, reproduced, or distributed to any person or entity without the written permission of the publisher.
Copyright 2023 Emond Montgomery Publications.