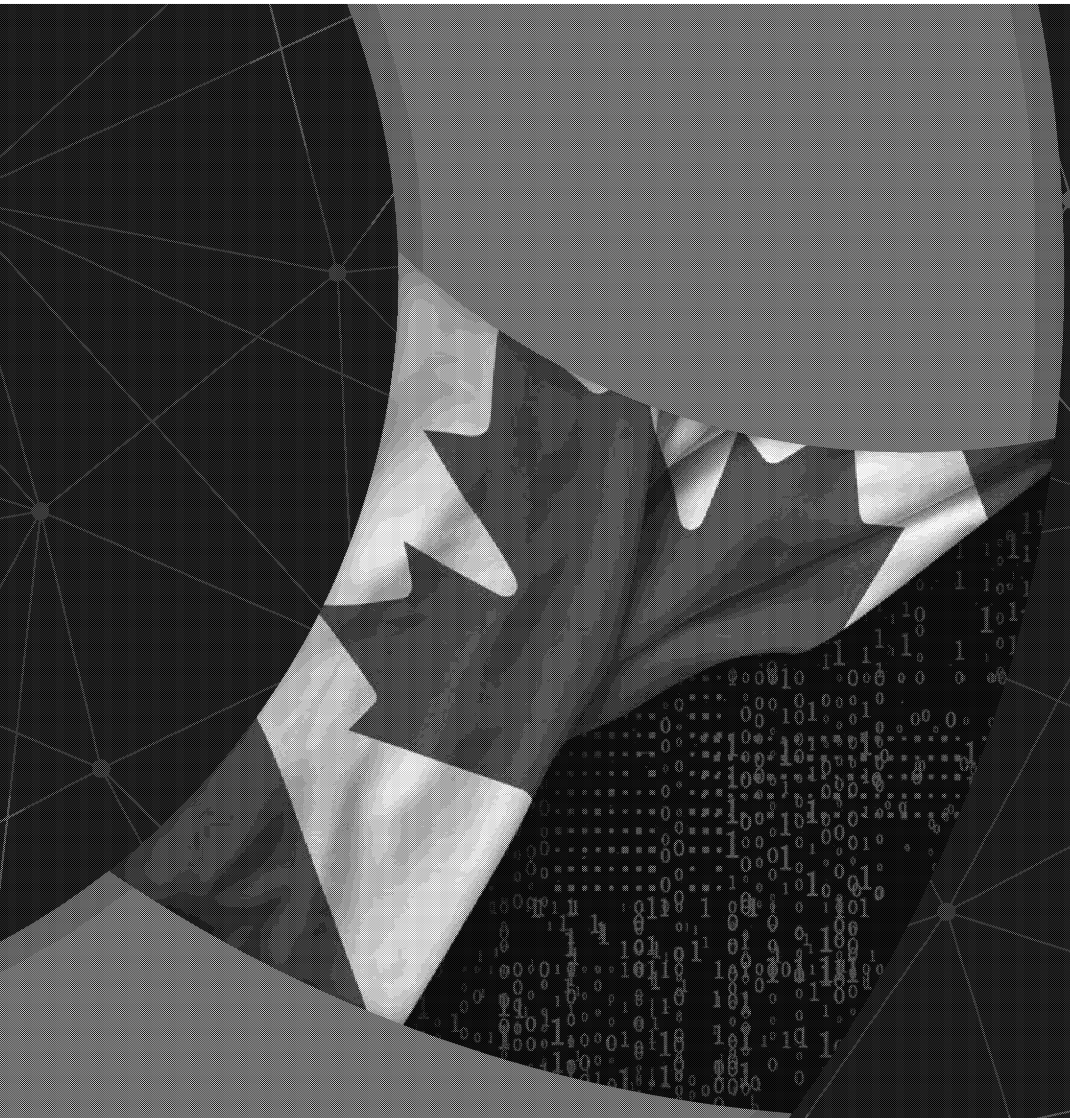


CANADIAN CENTRE FOR
CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT 2020

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

ABOUT THE CYBER CENTRE

The Canadian Centre for Cyber Security (Cyber Centre) is Canada's authority on cyber security. As part of the Communications Security Establishment (CSE), the Cyber Centre is a growing organization with a rich history. The Cyber Centre brought operational security experts from across the Government of Canada under one roof. In line with the National Cyber Security Strategy, the Cyber Centre represents a shift to a more unified approach to cyber security in Canada.

We are trusted experts in cyber security with a straightforward, focused mandate to collaborate with government, the private sector, and academia. We are builders, creators, developers, researchers, and scientists. We work to make Canada a safer place to be online.

WE HELP KEEP CANADA AND CANADIANS SAFE IN CYBERSPACE BY:

- Being a **clear, trusted source of relevant cyber security information** for Canadians, Canadian businesses, and critical infrastructure owners and operators;
- Providing **targeted cyber security advice and guidance** to protect the country's most important cyber systems;
- Working **side by side with provincial, territorial, and municipal governments, and private sector partners** to solve Canada's most complex cyber challenges;
- Developing and sharing our **specialized cyber defence technology and knowledge;**
- **Defending cyber systems**, including Government of Canada networks, by developing and deploying sophisticated cyber defence tools and technology;
- Leading the **Government's operational response during cyber events** by using our expertise and access to provide information immediately useful for managing incidents.

Cyber defence is a team sport. Our unique advantage helps make Canada more resistant to cyber threats and more resilient during and after cyber events.

LEARN MORE BY VISITING CYBER.GC.CA,
OR FOLLOW US ON TWITTER @CYBERCENTRE_CA

MINISTER'S FOREWORD

Cyber security is one of the most serious economic and national security challenges we face. Defending Canada and Canadians against cyber threats is a shared responsibility and a team effort. For anybody who thinks cyber security doesn't concern them, I would urge them to read this report.

I am grateful to the team at the Cyber Centre for this timely assessment. By sharing their insights, they are making sure policymakers, business leaders, and individual Canadians have the right information to counter these threats effectively.

We know that Canadians are among the most connected populations, and the COVID-19 pandemic has only increased and reinforced our reliance on the Internet. As we see almost daily in the headlines, cyber attackers are finding ever more sophisticated ways to exploit our connectivity.

Cyber threats are threats to the privacy, financial security, and even the personal safety of Canadians and the viability of Canadian businesses. "Cyber" just describes the delivery mechanism.

The Cyber Centre's unified approach to cyber security, which builds on Canada's already world-class cyber security expertise, can help Canadians rest assured that their government is prepared to meet the cyber security challenges of tomorrow, today.

The key findings of this report from the Cyber Centre are a timely reminder not to let our guard down.

We are seeing a proliferation of cyber threats, as sophisticated cybercriminals sell their tools and talent through illegal online markets.

Foreign state-sponsored cyber programs are probing our critical infrastructure for vulnerabilities.

Foreign efforts to influence public discourse through social media have become the "new normal".

More than that, the Internet is at a crossroads, with countries like China and Russia pushing to change the way it is governed, to turn it into a tool for censorship, surveillance, and state control.

By continuing to work with partners in government, business, and everyday Canadians, we can build a stronger, more cyber-resilient Canada.

Honourable Harjit Sajjan
Minister of National Defence

MESSAGE FROM THE HEAD OF THE CYBER CENTRE

It has been two years since the release of Canada's first National Cyber Threat Assessment 2018 (NCTA 2018), and during that time, much of what was predicted in 2018 has come to pass. The National Cyber Threat Assessment (NCTA 2020) comes at a time when Canadians and the Canadian economy have increasingly shifted their activities online, a shift that was made more rapid by the onset of COVID-19.

The COVID-19 pandemic has illustrated the extent to which the Canadian economy is reliant upon digital infrastructure. With a sudden increase in the number of Canadians working from home, the protection and security of cyber and telecommunications infrastructure, hardware and software, and the supply chains that support them, is critical to national security and economic prosperity. It is core to our daily lives and, in many cases, the digital infrastructure underpinning our society is out of view and hidden from most Canadians.

This document is not intended to review the NCTA 2018. Some predictions were accurate, others arrived at different speeds. It is said that hindsight is 20/20 and I challenged our assessment teams in 2018 and, again this year, in 2020, to be bold and make predictions. Only the future will tell if our predictions are accurate but they are informed by the full extent of CSE's expertise and knowledge of what is happening in the Canadian and worldwide cyber environment and leverage all sources of information both classified and available openly.

The NCTA is the foundation for many of the activities of the Canadian Centre for Cyber Security (Cyber Centre). The NCTA is intended to set our priorities. We work to address the threats outlined in this report and increase the overall cyber security baseline of Canada. But we don't do it alone. A good example of this approach is the partnership with the Canadian Internet Registration Authority (CIRA) and the launch of their Canadian Shield service. This service, made free to every Canadian by CIRA, can, if used, directly reduce the impact and reach of cybercrime, such as ransomware. Succinctly, it is a direct response to the statement in the NCTA 2018 that the threat most likely to impact Canadians is cybercrime.

But the last two years have also shown that doing the basics of cyber security matters. The vast majority of cyber incidents in Canada occurred because basic elements of cyber security weren't followed. For Canadians, you can rely upon GetCyberSafe.ca to provide simple, realistic, and achievable steps to make yourself more secure. If you are a Canadian not-for-profit, business of any size, or another level of government you can find information at cyber.gc.ca. We each need to do our part to make Canada more secure.

I hope you find NCTA 2020 informative and it spurs every Canadian to take even a single action to make themselves more secure. Each step contributes to our vision of a Secure Digital Canada.

Scott Jones
Head, Canadian Centre for Cyber Security

www.cyber.gc.ca

EXECUTIVE SUMMARY

Canadian individuals and organizations increasingly rely on the Internet for daily activities. In a COVID-19 context, this trend has accelerated to enable Canadians to work, shop, and socialize remotely in accordance with public health physical distancing guidelines. However, as devices, information, and activities move online, they are vulnerable to cyber threat actors.

Cyber threat actors pose a threat to the Canadian economy by exacting costs on individuals and organizations, notably through the theft of intellectual property and proprietary information. They threaten the privacy of Canadians through the theft of personal information, which facilitates additional criminal behaviour including identity theft and financial fraud. As physical infrastructure and processes continue to be connected to the Internet, cyber threat activity has followed, leading to increasing risk to the functioning of machinery and the safety of Canadians.

KEY JUDGEMENTS

- **The number of cyber threat actors is rising, and they are becoming more sophisticated.** The commercial sale of cyber tools coupled with a global pool of talent has resulted in more threat actors and more sophisticated threat activity. Illegal online markets for cyber tools and services have also allowed cybercriminals to conduct more complex and sophisticated campaigns.
- **Cybercrime continues to be the cyber threat that is most likely to affect Canadians and Canadian organizations.** We assess that, almost certainly, over the next two years, Canadians and Canadian organizations will continue to face online fraud and attempts to steal personal, financial, and corporate information.
- **We judge that ransomware directed against Canada will almost certainly continue to target large enterprises and critical infrastructure providers.** These entities cannot tolerate sustained disruptions and are willing to pay up to millions of dollars to quickly restore their operations. Many Canadian victims will likely continue to give in to ransom demands due to the severe costs of losing business and rebuilding their networks and the potentially destructive consequences of refusing payment.
- **While cybercrime is the most likely threat, the state-sponsored programs of China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.** State-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations.
- **State-sponsored actors are very likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure, such as the supply of electricity, to further their goals.** We judge that it is very unlikely, however, that cyber threat actors will intentionally seek to disrupt Canadian critical infrastructure and cause major damage or loss of life in the absence of international hostilities. Nevertheless, cyber threat actors may target critical Canadian organizations to collect information, pre-position for future activities, or as a form of intimidation.
- **State-sponsored actors will almost certainly continue to conduct commercial espionage against Canadian businesses, academia, and governments to steal Canadian intellectual property and proprietary information.** We assess that these threat actors will almost certainly continue attempting to steal intellectual property related to combatting COVID-19 to support their own domestic public health responses or to profit from its illegal reproduction by their own firms. The threat of cyber espionage is almost certainly higher for Canadian organizations that operate abroad or work directly with foreign state-owned enterprises.
- **Online foreign influence campaigns are almost certainly ongoing and not limited to key political events like elections.** Online foreign influence activities are a new normal, and adversaries seek to influence domestic events as well as impact international discourse related to current events. We assess that, relative to some other countries, Canadians are lower-priority targets for online foreign influence activity. However, Canada's media ecosystem is closely intertwined with that of the United States and other allies, which means that when their populations are targeted, Canadians become exposed to online influence as a type of collateral damage.

TABLE OF CONTENTS

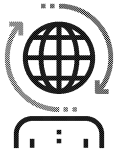
ABOUT THIS DOCUMENT

This document highlights the cyber threats facing individuals and organizations in Canada. It provides an update to the National Cyber Threat Assessment 2018 (NCTA 2018), with analysis of the interim years and forecasts until 2022. We recommend reading the NCTA 2020 along with the Introduction to the Cyber Threat Environment, which we have updated. This introduction provides a basic overview of cyber threat actors, their motivations, cyber tools, and an appendix of key cyber security tools and techniques referred to in this assessment.

As envisioned in the National Cyber Security Strategy, we prepared this document to help Canadians shape and sustain our nation's cyber resilience. It is only when we work together — government, the private sector, and the public — that we can build resilience to cyber threats in Canada.

LIMITATIONS

This assessment does not provide an exhaustive list of all cyber threat activity in Canada or mitigation advice. As a threat assessment, the purpose of this document is to describe and evaluate the threats facing Canada. We focus on understanding the current cyber threat environment and how threat activity can affect Canadians and Canadian organizations. General guidance can be found on the Cyber Centre's website in documents such as the Get Cyber Safe Campaign.



SOURCES

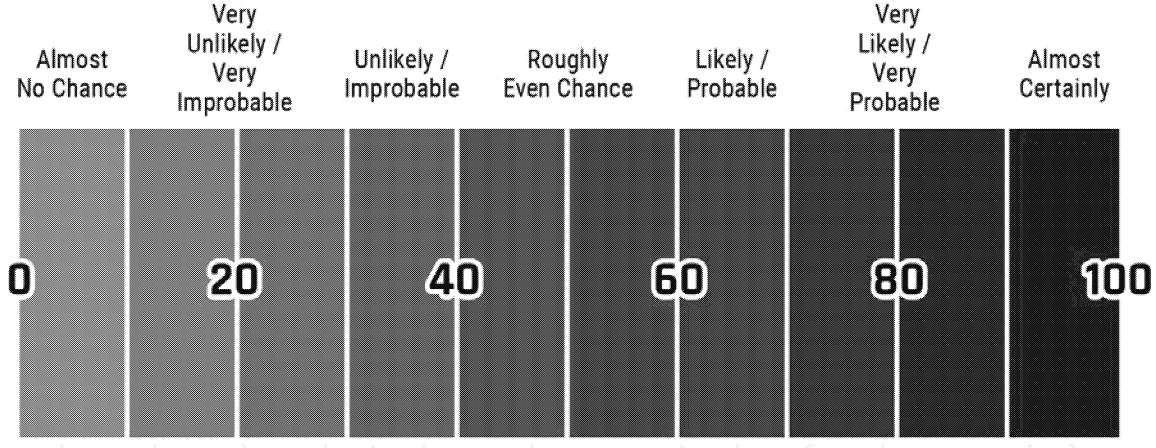
The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on the Cyber Centre's knowledge and expertise in cyber security. Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessment. CSE's foreign intelligence mandate provides us with valuable insights into adversary behaviour in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

ASSESSMENT PROCESS

Our cyber threat assessments are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases, and using probabilistic language. We use the terms "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly," "likely," and "very likely" to convey probability.

This threat assessment is based on information available as of 20 October 2020.

The chart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



AN EVOLVING CYBER THREAT LANDSCAPE

The National Cyber Threat Assessment 2018 (NCTA 2018) outlined the cyber threats faced by Canadian individuals, businesses, and critical infrastructure providers and predicted how the threats would evolve over the following years. Many of these judgements remain relevant. Cybercrime is still the most likely cyber threat to impact Canadians, state-sponsored cyber threat actors continue to conduct cyber espionage against Canadian organizations, including both businesses and critical infrastructure, and cyber threat actors continue to adapt and adopt more advanced methods. However, the cyber threats faced by Canadians have also evolved, keeping pace with the changing ways Canadians use technology and the Internet.

The Internet is indispensable to people around the world and to Canadians. Shifts in March 2020 due to the COVID-19 pandemic have quickly changed the cyber landscape, as more Canadians work, shop, and socialize remotely. We foresee this trend continuing, bringing more facets of Canadian economic, social, and political life online and exposing them to cyber threats, which have also been evolving to take advantage of the growing importance of the Internet and related technologies.

As a scene-setter for the rest of the assessment, we identify in the following section five trends that will drive the evolution of the cyber threat landscape.

TECHNOLOGY IS CHANGING SOCIETY AND ALTERING THE THREAT LANDSCAPE

Technological Changes Spur Societal Changes

Canadians are increasingly reliant on the Internet. More and more important day-to-day activities, such as banking, government services, health services, commerce, and education, have moved online for convenience and efficiency. In today's COVID-19 context, this trend has accelerated to allow Canadians to work, shop, and socialize remotely in accordance with public health physical distancing guidelines. These changes are driven by emerging and maturing technologies, which continue to create new ways to use the Internet that improve standards of living and change how individuals and organizations interact.

Technologies like artificial intelligence (AI), the Internet of Things (IoT), the Industrial Internet of Things (IIoT), and cloud computing underpin a wide range of personal, commercial, and industrial activities. Advancements in the next two years in these and other information technologies, such as the roll out of 5G global wireless telecommunications, will change how Canadians do business, operate industrial plants, buy and obtain consumer goods, receive medical care, and more. In turn, Canadians will continue to see changes in other areas of their lives, including the design of cities and modes of transportation and the undertaking of elections and other democratic processes.

The Threat Landscape

As devices, information, and activities valued by Canadian individuals and organizations are moved online, they become susceptible to threat activity. Cyber threat actors—particularly cybercriminals and state-sponsored actors—continue to adapt their activities to find information that Canadians value and attempt to obtain it, hold it for ransom, or destroy it.

We judge that cybercriminals, who are motivated by financial gain, almost certainly represent the most pervasive cyber threat to Canadians. They conduct the most threat activities against Canadians, including ransomware attacks, theft of personal, financial, and confidential information, and distributed denial of service (DDoS) attacks. As discussed below, illegal markets for cyber products and services allow cybercriminals to access more sophisticated cyber tools.

However, the most sophisticated capabilities belong to state-sponsored cyber threat actors who are motivated by economic, ideological, and geopolitical goals. Their activities include cyber espionage, intellectual property theft, online influence operations, and disruptive cyber attacks.

We assess that almost certainly the state-sponsored programs of China, Russia, Iran, and North Korea pose the greatest state-sponsored cyber threats to Canadian individuals and organizations. However, many other states are rapidly developing their own cyber programs, benefiting from various legal and illegal markets to purchase cyber products and services.

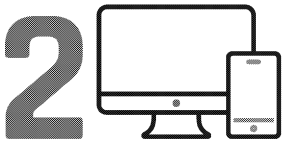
Activities by hacktivists or thrill-seekers almost certainly pose a less common and less sophisticated threat to Canadians. In general, activities by both hacktivists and thrill-seekers are less common than other types of activity, and these threat actors often have fewer resources to devote to their activities, limiting the sophistication of their operations. Hacktivists have conducted newsworthy cyber activities in 2020. One of these incidents primarily targeted US victims but also impacted entities in Canada, exposing data belonging to 38 Canadian police agencies.[1]

Below we identify five trends that will drive the evolution of the cyber landscape and threat activity.

MORE PHYSICAL SAFETY OF CANADIANS IS BEING PUT AT RISK

The safety of Canadians depends on critical infrastructure (e.g., energy, water), as well as consumer and medical goods (e.g., cars, home security systems, pacemakers, etc.), many of which are controlled by computers embedded within them. Increasingly, these computers are being connected to the Internet by their manufacturers, sometimes unbeknownst to consumers, to enable new features or provide data to a third party. However, once connected, these infrastructures and goods are susceptible to cyber threat activity, and maintaining their security requires investments over time from manufacturers and owners that can be difficult to sustain.

An important part of this trend is operational technology (OT), which is a broad term that refers to technology used to control physical processes such as dam openings, boiler activities, electricity conduction, and pipeline operations. In contrast with Information Technology (IT)—such as hardware and software found in most homes and organizations—OT has been relatively protected from cyber threat activity, because it was not originally designed to be connected to the Internet. However, manufacturers are now converging IT and OT. These changes are meant to increase efficiency and support long-term planning, but they also increase the risk of cyber threat activity reaching OT systems. A 2019 survey found that 68% of manufacturers plan to increase their investment in IT-OT convergence solutions for their organizations over the next two years.[2] We assess that, almost certainly, the most pressing threats to the physical safety of Canadians are to OT and critical infrastructure. However, in the future, targeting of smart cities and IoT devices such as personal medical devices and Internet-connected vehicles, may also put Canadians at risk.



MORE ECONOMIC VALUE IS BEING PUT AT RISK

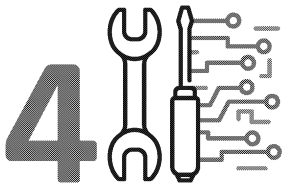
As we noted in NCTA 2018, state-sponsored cyber threat actors and cybercriminals continue to exact costs from Canadian individuals and businesses and damage the economy. Cybercriminals defraud individuals and companies and extort money from them through ransomware, and state-sponsored threat actors steal intellectual property and proprietary business information. Additionally, an increasing number of Canadians have moved their financial activity online, thereby increasing their susceptibility and attractiveness to cybercriminals. In 2019, 94% of Canadians had home Internet access (up from 79% in 2010) and 71% of Canadians banked online (up from 67% in 2010).[3]

Due to restrictions related to the COVID-19 pandemic, Canadians have shifted quickly and significantly towards remote work arrangements. They are accessing intellectual property and other sensitive data using personal devices and home Wi-Fi networks that are often poorly secured in comparison to corporate IT infrastructure. The protection of intellectual property is crucial to the productivity and competitiveness of Canadian companies, and vital for Canada's economic growth and national defence. Certain countries continue to use advanced cyber espionage programs to obtain unfair advantages in the global marketplace and to improve their military technology. Commercial cyber espionage against Canadian companies is ongoing across a range of fields including aviation, technology and AI, energy, and biopharmaceuticals.[4]

MORE COLLECTED DATA INCREASES PRIVACY RISK

Canadians generate an incredible amount of data about their locations, shopping habits, patterns of life, and personal health when they use their phones and computers, bank and shop online, wear their smart watches and fitness trackers, arm their home security systems, or monitor their insulin levels with smart medical devices. As Canadians generate, store, and share more personal information online, this data becomes vulnerable to cyber threat actors via breaches or misuse by the companies or foreign governments that collect it. The growth in Internet-connected devices has also added to the amount of data collected on Canadians. The Office of the Privacy Commissioner of Canada (OPC) recorded 680 data breaches impacting 28 million Canadians in the year ending on 1 November 2019.[5]

Meanwhile, advances in data science make it more difficult to maintain data anonymity and privacy protections. These technological advances can allow information that was previously anonymous to be linked to other datasets and de-anonymized. Data privacy is an issue of importance for Canadians. A study commissioned by the OPC found that 92% of Canadians expressed concern about the protection of their privacy, with 37% stating that they were extremely concerned.[6]



4 ADVANCED CYBER TOOLS AND SKILLS ACCESSIBLE TO MORE THREAT ACTORS

An Increasing Commercial Market for Cyber Tools and Talent

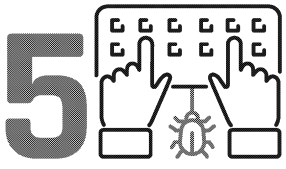
The commercial sale of cyber tools coupled with a global pool of talent has resulted in more threat actors and more sophisticated threat activity, which increases the challenges inherent in identifying, attributing, and defending against cyber threat activity. Commercial markets for tools and talent have resulted in a shortening of the time it takes for a state to build a cyber program and an increase in the number of states with cyber programs. The Council on Foreign Relations maintains a growing list of countries suspected of sponsoring cyber operations since 2005. The current list stands at 33 countries.[7]

The global market for cyber products and services is projected to grow from approximately $204 billion CAD in 2018 to $334 billion CAD in 2023.[8] State-sponsored threat actors are recruiting skilled expatriates with lucrative salaries as a way to rapidly develop their national cyber programs. This is a significant change from when states had to develop their own cyber talent pipeline and build their own tools.

A Blossoming Cybercrime Ecosystem

In addition to a large legitimate commercial market, there is also an illegal market for cyber tools and services. Many online marketplaces allow vendors to sell specialized cyber tools and services that users can purchase and use to commit cybercrimes, including website defacement, espionage, DDoS attacks, and ransomware attacks. Purchasing tools and services greatly reduces the start-up time for cybercriminals and enables them to use better tools.

The development of cryptocurrency has facilitated the activities of cybercriminals and states as a means of exchanging and laundering money with greater anonymity. Without cryptocurrencies, many forms of cybercrime would be cost-prohibitive for cybercriminals. Anti-money laundering laws have been implemented in many countries to counter cybercrime. However, the success of cybercriminals is partially dependent upon jurisdictions in states around the world with lenient or non-existent laws and law enforcement related to cybercrime. For example, in Russia, China, and Iran, cybercriminals are very unlikely to be prosecuted for financially motivated cyber threat activity against targets outside of the country.[9]



5 INTERNET AT A CROSSROADS

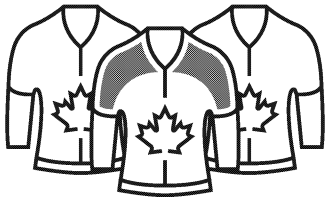
Internet Governance

Many states are pushing hard to change the accepted approach to Internet governance from the multi-stakeholder approach to one of state sovereignty. They view ideas and information primarily through the lenses of domestic stability and national security and want an Internet that will allow them to track their citizens and censor information. Some of these regimes use the Internet to quell protests, arrest dissidents, feed their citizens misinformation, and surveil them.[10] The leaders of the state-sovereignty governance model, China and Russia, continue to push their agenda in international forums such as the International Telecommunications Union (ITU) and other UN bodies, via policy proposals and technical standards proposals. Technical standards can have extraordinary real-world implications, as can be seen in the New Internet Protocol (NIP) proposal made by China and Chinese telecommunications companies, as the NIP would fundamentally transform the way the Internet works.[11] The NIP would provide certain cyber security advantages, but it would enable powerful censorship, surveillance, and state control.[12]

Historically, the dominant approach to Internet governance has been the multi-stakeholder approach championed by Canada and like-minded countries, that includes wide participation from governments, industry, civil society, and academia meeting across a range of bodies that establish technical and policy guidelines. This approach views the Internet as a global development tool that must balance universal access and interoperability with privacy and security.

Online Foreign Influence

As we noted in our Cyber Threats to Canada's Democratic Process Assessment, adversaries use online influence to further their core interests, which typically consist of national security, economic prosperity, and ideological goals. Online foreign influence activities have become a new normal, and adversaries seek to influence domestic events like elections as well as impact international discourse related to current events. Online democratic engagement requires a fair, open Internet, free from manipulation by foreign actors. An increasing number of states have developed cyber tools and are using them to carry out large-scale online influence activities. They exploit social media and legitimate advertising and information-sharing tools to reach a large audience and make their messaging more effective. Deepfake technology—allowing the creation of realistic-looking videos of events and public figures—adds another layer of uncertainty and confusion for the targets of disinformation campaigns. Deepfake technology has developed rapidly, with the industry expanding to include various face swapping applications, products that can produce a video of a full person from scratch[13], and audio deepfake software that is capable of cloning existing human voices.[14]



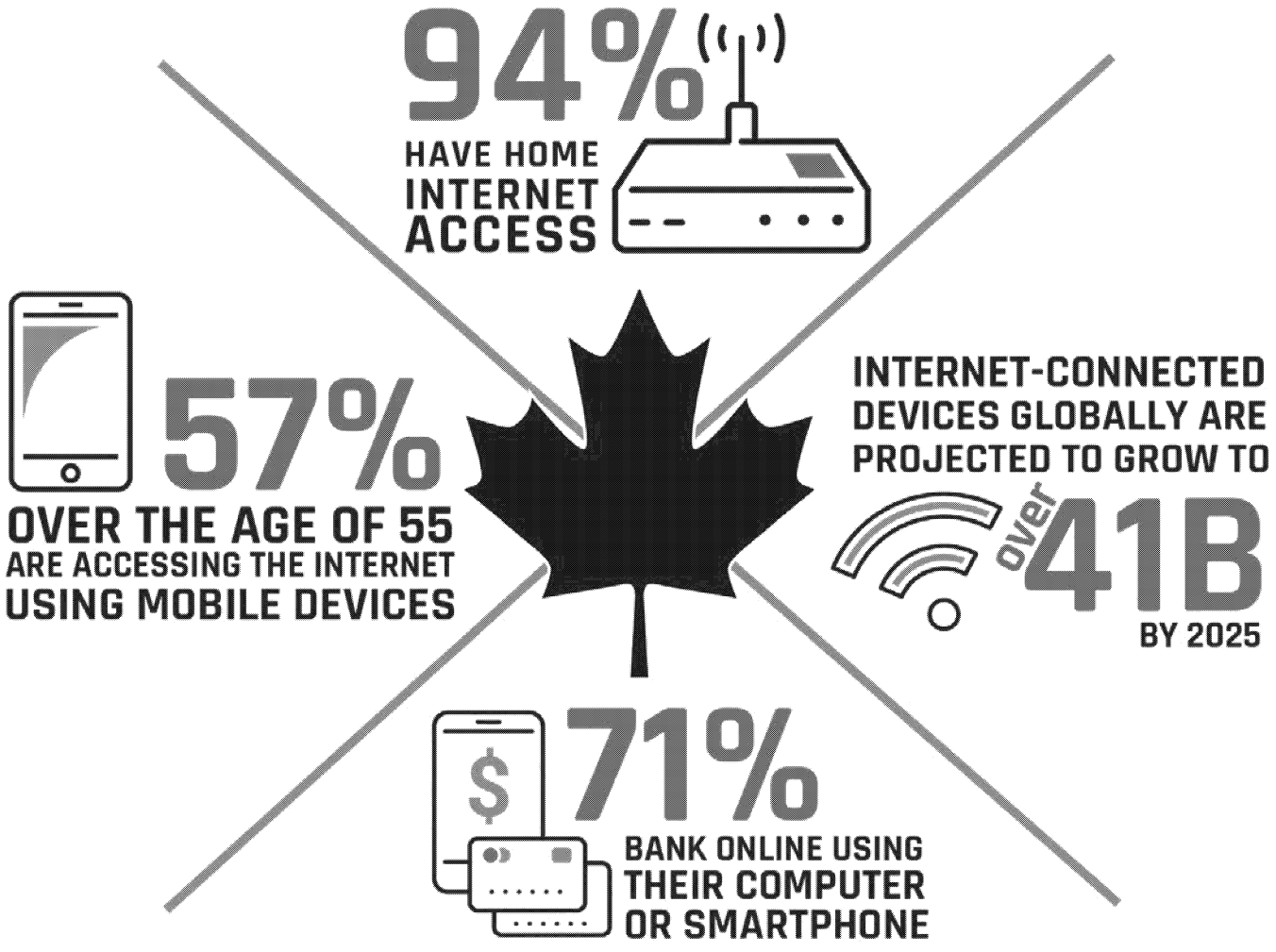
CYBER THREATS TO CANADIAN INDIVIDUALS

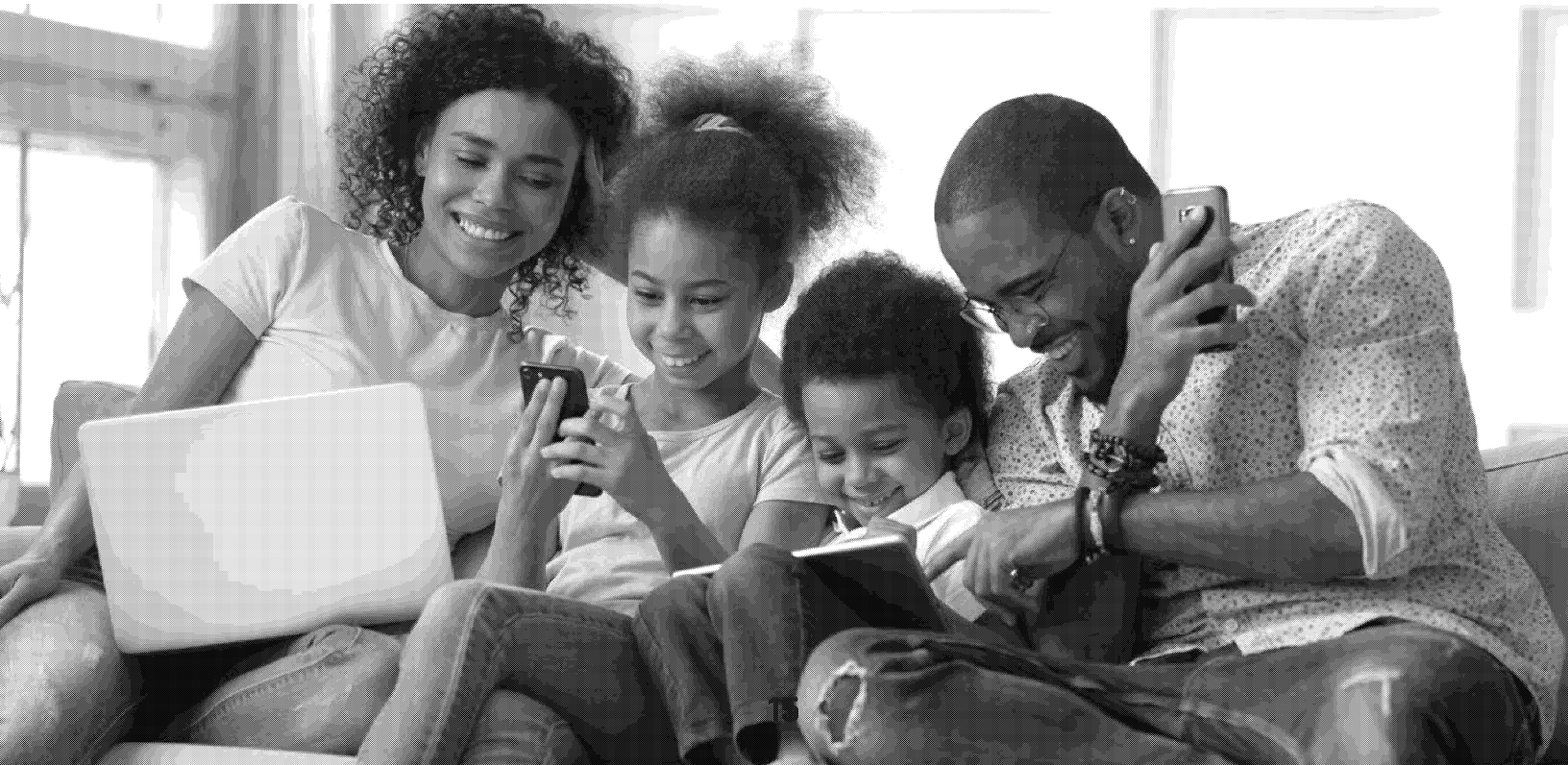
Canadians are putting more of their personal information online, and they increasingly depend on Internet-connected devices for communication, finances, entertainment, comfort, and safety. As technology and habits change, cyber threat actors adapt quickly to take advantage of new opportunities and keep pace with current events, including modifying cyber threat activity during the COVID-19 pandemic.

Canadians continue to fall victim to online fraud schemes. As mentioned in NCTA 2018, we assess that cybercrime will almost certainly continue to be the cyber threat that Canadians are most likely to encounter. Since NCTA 2018, cyber threat actors have improved their ability to keep scams relevant and appealing by associating their cyber fraud operations with current events. Elections, tax season, and trending news stories have all been used as a backdrop for cybercrime. For example, threat actors have leveraged the COVID-19 pandemic to trick victims into clicking on malicious links and attachments. Cyber threat actors also steal financial, medical, and other personal information to sell online or use in cybercrimes. Large corporate data breaches impact millions of customers and reveal personal information that can be used in follow-on crimes.

Canadians also continue to be subjected to online foreign influence operations that seek to influence Canadian public opinion and political discourse. Finally, evolving technologies like IoT medical devices, Internet-connected vehicles, and smart home security systems provide new targets for cyber threat actors to threaten the physical safety of Canadians.

Figure 1: Canadian Internet Usage, from 2018 Canadian Internet Use Survey by Statistics Canada[15], 2019 CIRA Internet Factbook [16], and forecasts of the International Data Corporation[17]





FRAUD AND EXTORTION

Individual Canadians lost over $43 million CAD to cybercrime fraud in 2019, according to statistics from the Canadian Anti-Fraud Centre.[18] This number only accounts for the reported cases of cybercrime fraud, and we assess that it is almost certain that actual amounts are higher. As predicted in NCTA 2018, over the last two years, we have observed increasingly sophisticated cyber fraud and extortion attempts directed at Canadians. We assess that this trend will almost certainly continue, facilitated by cybercrime marketplaces that enable threat actors to purchase cybercrime tools and services.

One way that cyber threat actors conduct fraud is by posing as legitimate organizations, such as government institutions, banks, or law firms to trick Canadians into clicking on malicious links or attachments which download malware onto their devices. For example, scammers create fake websites and online ads that offer cheap immigration services or may even guarantee high paying jobs for new immigrants. Many of the websites look like official government sites but require the victim to pay a fee to access "important forms".[19] Since March 2020, the Cyber Centre has worked with partners to take down over 3,500 websites, social media accounts, and email servers that were fraudulently representing the Government of Canada.

Cyber threat actors also extort money from victims by threatening cyber attacks or by stealing or claiming to have stolen incriminating information from victims. Threat actors also create fake profiles on social media and dating websites, which they use to lure victims into an online relationship that facilitates extortion and fraud. In some cases, they obtain intimate videos of their victim and then threaten to send the video to the victim's contacts unless they receive payment.[20]

THREAT ACTORS LEVERAGE A GLOBAL CRISIS – COVID-19

In 2020, we have observed cyber threat actors developing COVID-19-related content to trick victims into clicking on malicious links and attachments. Cyber threat actors know that people are anxious about the future and are less likely to act prudently when presented with emails, SMS messages, or advertisements related to COVID-19.

COVID-19 lures often attempt to replicate or imitate the branding and style of legitimate organizations, such as international organizations and public health agencies. Cyber threat actors can produce convincing copies of government websites and official correspondence. One SMS phishing campaign claimed to provide access to a Canadian Emergency Response Benefit payment, but only after the target divulged personal financial details. Another campaign impersonated the Public Health Agency of Canada's Medical Officer of Health to deliver malware through a fake COVID-19 update that appeared official and legitimate.

Figure 2: The Elements of Malicious Communication

THREATS TO PRIVACY

In NCTA 2018, we described how financial and personal information is attractive to cybercriminals and how they can exploit stolen information for financial gain. This remains true, but the threat has increased due to the growing quantity of information that is stored online as well as improvements in data science that enable new methods for exploiting stolen personal, financial, and even medical information.

In addition, cybercriminals are not the only cyber threat actors interested in this data: state-sponsored actors have also been observed compromising large databases to advance national priorities.

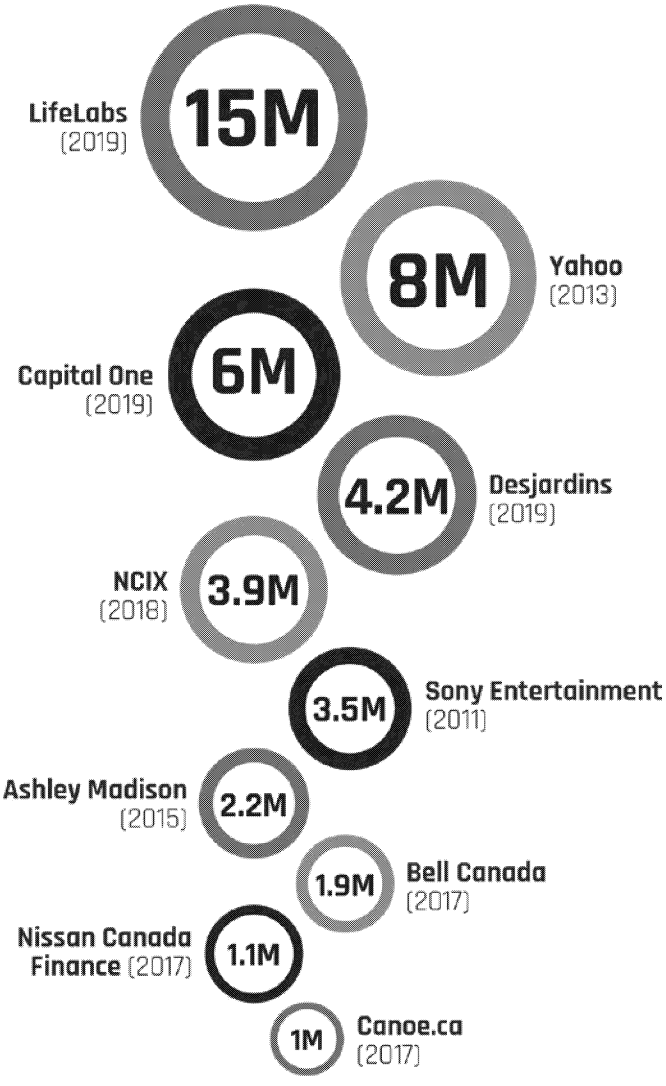
Financial Information

As more information is shared and stored online, the threat to individual privacy increases. Data breaches threaten the financial information of Canadians that is held by businesses which fall prey to cyber threat actors. Stealing personal and financial information from Canadians is profitable for cybercriminals, and we assess that it will likely increase in the next two years.

Cybercriminals profit by obtaining login credentials, credit card details, and other personal information and then using this information to steal money, commit fraud, or sell it on cybercrime marketplaces. In June 2019, the data breach of Canadian financial services company Desjardins affected the records of 4.2 million of its Canadian customers.[21] Personal information including names and birthdates, social insurance numbers, contact information, and banking details were compromised.

A similar event against another financial institution, Capital One, occurred in March 2019, exposing the personal information of 6 million Canadian customers. The stolen data included personal information in addition to credit scores, transaction data, and bank account numbers.[22]

Figure 3: Ten of the Largest Data Breaches Impacting Canadians, 2011 to Present, by number of records



CRYPTOCURRENCY AND CRYPTOJACKING

Cybercriminals use malware to take unauthorized control of the processing power of computers to generate or "mine" cryptocurrency. This is called cryptojacking. Out-of-date or unpatched systems are particularly vulnerable to cryptojacking and some owners may be completely unaware that their device has been compromised, while others may experience slower performance or a rapidly drained battery.[23]

As we predicted in the 2018 NCTA, we have seen cybercriminals continue to develop and deploy malware in cryptojacking operations. We assess that this activity will very likely continue in the next two years, with activity levels linked to the fluctuations in cryptocurrency values.

Medical and Personal Data

In 2019, medical laboratory testing firm LifeLabs was the victim of a cyber breach that compromised the sensitive personal and medical information of 15 million Canadians before the lab paid a ransom to retrieve the information.[24] Threat actors, particularly state-sponsored cyber actors, are using data science to make better use of large datasets. They can identify, profile, and track individuals by combining and de-anonymizing data from multiple datasets.

Stolen personal data can be used by cyber threat actors for credential stuffing, where large numbers of compromised pairs of usernames and passwords are entered into websites in the hopes that one will match an existing account on the site. Stolen personal data can include credentials that allow this type of activity as well as access to the answers to personal security questions, rendering this protection ineffective. After collecting data from multiple breaches, cybercriminals may be able to combine the available personal information on an individual and more effectively target cyber threat activity.

CAPITAL ONE AND MARRIOTT BREACHES

The accumulation of data attracts both cybercriminals and state-sponsored cyber threat actors. In 2019, a cybercriminal stole customer data from US financial services firm Capital One. The breach affected 106 million individuals, including six million Canadians, and collected private data including social insurance/security numbers and bank account details.[25] In 2018, Marriott Hotels announced that its reservation system had been breached, and that private data on about 500 million guests was stolen. The attack was linked to state-sponsored hackers and allowed them to collect data including names, addresses, and passport numbers.[26]

ONLINE FOREIGN INFLUENCE

A growing number of states have built and deployed programs dedicated to undertaking online influence as part of their daily business. Adversaries use online influence campaigns to attempt to change civil discourse, policymakers' choices, government relationships, and the reputation of politicians and countries both nationally and globally. They try to delegitimize the concept of democracy and other values such as human rights and liberty, which may run contrary to their own ideological views. They also try to exacerbate existing friction in democratic societies around various divisive social, political, and economic issues. While online foreign influence activities tend to increase around elections, these ongoing campaigns have broadened in scope since 2018, expanding to react and adapt to current events, shifting their content strategies around trending news stories and popular political issues.

As predicted in NCTA 2018, Canadians have continued to be the subject of online foreign influence activity. For instance, we have observed recent campaigns focus their content around COVID-19 and government responses to the pandemic. Disinformation campaigns have also sought to discredit and criticize Canadian politicians to damage their reputations. However, we assess that relative to some other countries, Canadians are lower-priority targets for online foreign influence activity, though Canada's position on high-tension geopolitical issues could increase the threat. Crucially, Canada's media ecosystems are closely intertwined with those of the United States and other allies, which means that when their populations are targeted, Canadians become exposed to online influence as a type of collateral damage.

We assess that Canadians' exposure to online foreign influence is almost certainly going to continue for the next two years or more, though threat actors will be forced to adapt their activities to the changing policies of Internet companies such as Google, Facebook, and Twitter.

STATE-SPONSORED ACTORS SEEKING TO DIVIDE CANADIANS

Analysis of publicly released Twitter data revealed that Russian and Iranian online trolls used fraudulent Twitter accounts to highlight divisions among Canadians by amplifying inflammatory arguments surrounding divisive political issues such as terrorism, climate change, pipeline construction, and policies on immigration and refugees. Many of these tweets reacted to major news events such as the January 2017 Quebec City mosque shooting and the June 2019 approval of the Trans Mountain Pipeline expansion project.[27]

THREATS TO PHYSICAL SAFETY AND SECURITY

Personal Internet-connected devices, including IoT medical devices, Internet-connected vehicles, and smart home security systems are being integrated into day-to-day life and providing new targets for cyber threat actors. While other cyber threats, such as data breaches, are more common and have broader impacts, there is a risk that future cyber threat activity against these devices and systems can impact physical safety. For example, Internet-connected medical devices are increasingly common and are vulnerable to cyber threat actors who could target these devices and degrade or disrupt their performance.

As another example, stalkers and abusive partners are taking advantage of vulnerabilities in personal IoT devices to steal information collected by fitness trackers and smart home technologies to identify and locate their victims. They are also manipulating smart home devices to control a victim's surroundings and intimidate them. In one case, a man operated a smart vehicle application that allowed him to stop, start, and track his victim's vehicle from his phone.[28] An organization providing support for victims of domestic abuse reported that, as of January 2019, more than 2,500 of its clients had reported experiences of technology-facilitated abuse.[29]

INTERNET-CONNECTED PERSONAL MEDICAL DEVICES

In March 2020, Health Canada issued an alert that medical devices, such as pacemakers, blood glucose monitors, and insulin pumps with a particular Bluetooth chip were vulnerable to cyber attacks that could crash the device, unlock it, or bypass security to access functions that should only be available to an authorized individual.[30]

CYBER THREATS TO CANADIAN ORGANIZATIONS

As we predicted in NCTA 2018, cybercrime remains the most common threat faced by Canadian organizations of all sizes. However, other cyber threat activity, such as cyber espionage, can have a greater impact. Information stolen by cyber threat actors can be held for ransom, sold, or used to gain an unfair competitive advantage. Over the past two years, targeting of industrial processes and ransomware attacks have become regular occurrences resulting in major impacts, including reputational damage, productivity loss, legal repercussions, recovery expenses, and damage to infrastructure and operations. We assess that ransomware directed against Canada in the next two years will almost certainly continue to target large enterprises and critical infrastructure providers.

Cyber threat actors also put the information held by Canadian organizations at risk, including intellectual property as well as customer and client data. The theft of this information can have both short- and long-term financial consequences for the victims, including impacts to global competitiveness and reputational damage. During the COVID-19 pandemic, state-sponsored cyber threat actors have targeted Canadian intellectual property related to combatting COVID-19, and we assess that it is almost certain that state-sponsored actors will continue to do so in order to support their own domestic public health responses or to profit from its illegal reproduction by their own firms.

Cyber threat actors also exploit trusted business relationships between Canadian organizations, target both online and in-person payment systems, exploit supply chain vulnerabilities, and take advantage of the privileged access managed service providers maintain into the networks of their clients. These activities can be used to defraud organizations, conduct ransomware attacks, or steal proprietary information or customer and client data.

Canadian organizations of all sizes, such as small- and medium-sized enterprises, municipalities, universities, and critical infrastructure providers, face a growing number of cyber threats.[31]

These organizations control a range of assets that are of interest to cyber threat actors, including intellectual property, financial information and payment systems, data about customers, partners and suppliers, and industrial plants and machinery. As a general rule, the more Internet-connected assets an organization has, the greater the cyber threat it faces.

Figure 4: List of Assets Owned by Organizations that can Increase Cyber Security Risk

TARGETING THE SAFETY OF CANADIANS

Targeting Industrial Control Systems and Critical Infrastructure

The safety of Canadians is at risk when cyber threat actors target organizations responsible for the operation of utilities, delivery of healthcare, or provision of essential government services. However, as we judged in NCTA 2018, we assess that it remains very unlikely that cyber threat actors will intentionally seek to disrupt Canadian critical infrastructure and cause major damage or loss of life in the absence of international hostilities. Nevertheless, cyber threat actors may target critical Canadian organizations to collect information, pre-position for potential future activities, or as a form of intimidation. We judge that state-sponsored actors are very likely attempting to develop the additional cyber capabilities required to disrupt the supply of electricity in Canada.

Industrial control systems (ICS) are a type of OT that monitors and controls physical equipment in industrial or critical infrastructure processes. Especially in the electricity sector, ICS are targeted across the world, mostly by state-sponsored cyber threat actors. In 2019, Russia-associated actors probed the networks of electricity utilities in the US and Canada.[32] Iranian hacking groups have targeted ICS infrastructure in rival nations, including the US, Israel, and Saudi Arabia.[33] North Korean malware has been found in the IT networks of Indian power plants, and US utility employees have been targeted by Chinese state-sponsored cyber threat actors.[34]

In recent years, ransomware has increasingly impacted ICS. We assess that ransomware has almost certainly improved its ability to spread through corporate IT networks and threaten adjacent ICS environments. In some cases, victims have chosen to disable their industrial processes as a precautionary measure during a significant ransomware event. For example, in March 2019, a Norwegian aluminum company was impacted by a ransomware event that disrupted its logistical and production data so severely that it prompted the shutdown of ICS control and reversion to manual operations.[35] We assess that cybercriminals will very likely increase their targeting of ICS in the next two years in an attempt to place increased pressure on critical infrastructure and heavy industry victims to promptly accede to ransom demands.

ICS RANSOMWARE IN ACTION

Since January 2019, at least seven ransomware variants have contained instructions to terminate ICS processes.[36] The impact of these attacks on ICS varies according to the specific circumstances of the industrial process and the reaction of the site staff.[37] In June 2020, a car manufacturer halted production at most of its North American plants, including one in Canada, "to ensure safety" after very likely being hit by one of these ransomware variants.[38]

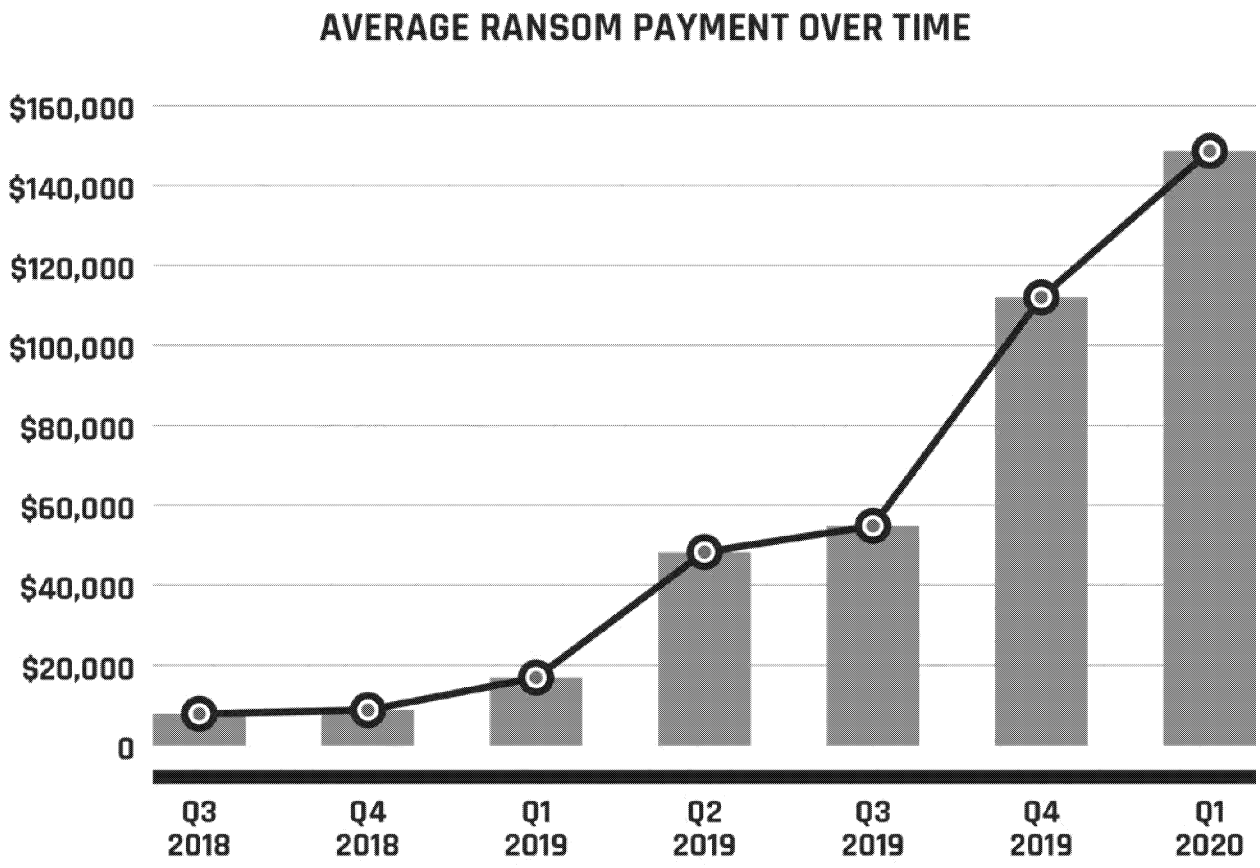
THREATS TO CANADIAN FINANCIAL AND ECONOMIC HEALTH

Cyber threat activity results in unwanted expenses for organizations, including the costs of ransoms or stolen funds, losses due to the disruption of operations, the price of securing and insuring networks, reputational damage and related loss of customers, and theft of intellectual property or confidential information.[39] These costs are a drain on organizations' finite resources and decrease their competitiveness against other companies. Taken together, they are also a drain on the Canadian economy.

Ransomware and Big Game Hunting

NCTA 2018 identified ransomware as the most common form of malware used for extortion against Canadian individuals. While it has remained prevalent, cybercriminals have shifted their tactics to allow them to increase their ransom demands and increase the likelihood of success. In recent years, cybercriminals have increasingly engaged in big game hunting (BGH), focusing their activities against large enterprises that will not tolerate sustained disruptions to their networks and are willing to pay large ransoms to quickly restore their operations.[40] As BGH ransomware campaigns have become more common, the value of ransom demands has increased. Ransomware researchers estimate that the average ransom demand increased by 33% since Q4 2019 to approximately $148,700 CAD in Q1 2020 due to the impact of targeted ransomware operations.[41] At the more extreme end of the spectrum are multi-million-dollar ransom events, which have become increasingly common. In October 2019, a Canadian insurance company paid $1.3 million CAD to recover 20 servers and 1,000 workstations.[42] In addition, we assess that it is likely that state-sponsored cyber threat actors will use ransomware to obfuscate the origins or intentions of their cyber operations. It is almost certain that the intelligence services of multiple countries maintain associations with cybercriminals that engage in ransomware schemes. In these mutually beneficial relationships, cybercriminals share stolen data with intelligence services while the intelligence service allows the cybercriminals to operate free from law enforcement.

Figure 5: Average Ransomware Payments, 2018 to 2020 (data from Coveware converted from USD to CAD)[43]



We expect that ransomware directed against Canada in the next two years will almost certainly continue to target large enterprises and critical infrastructure providers. Furthermore, many Canadian victims will likely continue to give in to ransom demands due to the severe economic and potentially destructive consequences of refusing payment. Since late 2019, multiple Canadian businesses and provincial governments have had their data publicly leaked by ransomware operators for refusing payment, including a construction company and a consortium of Canadian agricultural companies.[44]

RANSOMWARE FREQUENTLY TARGETS THE HEALTH SECTOR

In 2019 and 2020, many Canadian health organizations have been targeted in ransomware attacks. For example, three Ontario hospitals were the victims of ransomware attacks in October 2019, and a Canadian diagnostic and specialty testing company was compromised by ransomware in December 2019. In early 2020, ransomware also targeted a medical company in Saskatchewan.[45] During the COVID-19 pandemic, many health sector organizations globally have experienced ransomware attacks, including hospitals and healthcare centres in the Czech Republic, the US, Spain, and Germany.[46] Health sector organizations are popular ransomware targets because they have significant financial resources and network downtime can have life-threatening consequences for patients, increasing the likelihood that victims will pay the ransom.

Stealing Intellectual Property and Proprietary Information

In NCTA 2018, we described the threat posed to Canadian businesses by commercial cyber espionage, and this threat remains today, with state-sponsored cyber threat actors continuing to conduct cyber espionage against the networks of organizations in Canada and allied nations, seeking intellectual property, trade secrets, and other commercially sensitive information. In Canada, these threat actors have conducted espionage against a wide variety of Canadian organizations including businesses, academia, and governments, especially organizations in the health and biotechnology, energy, telecommunications, and defence sectors.[47]

A long-running campaign by state-sponsored cyber threat actors used compromised managed service providers (MSPs) to target intellectual property and confidential business and technological information related to aviation, telecommunications, health and biotechnology, and other sectors. They targeted companies in Canada as well as at least 12 other countries since 2006.[48] In 2019, it was reported that one state-sponsored campaign targeted over two dozen universities in Canada, the US, and Southeast Asia in an attempt to acquire information related to military-use maritime technology and research.[49]

During the COVID-19 pandemic, large medical and biopharmaceutical companies in Canada and abroad have been targeted by state-sponsored cyber threat actors attempting to steal intellectual property related to COVID-19 tests, treatments, and vaccines. We assess that it is almost certain that state-sponsored actors will continue attempting to steal Canadian intellectual property related to combatting COVID-19 in order to support their own domestic public health response or to profit from its illegal reproduction by their own firms.[50]

Organizations with overseas activities and infrastructure face additional cyber threats. Their operations abroad may be governed by different, and sometimes weaker, intellectual property, privacy, or national security laws. Many countries have the legal authority and technical ability to covertly access data when it transits or resides in their country. This has implications for Canadian data and intellectual property that is sent abroad to offices in other states or that transits networks in other countries. Even data that is sent between two entities located in Canada may transit foreign networks as part of the path to their destinations. However, consistent with our judgement in NCTA 2018, we assess that the threat of cyber espionage is almost certainly higher for Canadian organizations that operate abroad or work directly with foreign state-owned enterprises.

RUSSIAN ACTORS TARGETING COVID-19 VACCINE RESEARCH

In July 2020, the Cyber Centre, the UK National Cyber Security Centre, and the US National Security Agency released a joint advisory reporting on the tactics, techniques, and procedures of a state-sponsored cyber threat actor targeting organizations involved in COVID-19 vaccine development in Canada, the US, and the UK.[51] We assess that the cyber threat actor responsible is almost certainly part of the Russian intelligence services and highly likely wishes to steal information and intellectual property relating to the development and testing of COVID-19 vaccines.

Stealing Customer and Client Data

As predicted in NCTA 2018, cyber threat actors continue to target large datasets held by organizations located in Canada and around the world. Large databases containing personal information such as names, addresses, phone numbers, employment information, credentials, and financial details are valuable to cyber threat actors. The aggregation of data collected from multiple breaches can provide cybercriminals with enough information to fraudulently apply for loans or credit cards, file false tax returns, transfer money illegally, extort victims, gain access to online accounts, or engineer persuasive phishing emails.[52] This data can also be used by state-sponsored cyber actors to pursue dissidents, minorities, or espionage targets within their country or abroad.

Data theft by cybercriminals tends to be opportunistic and financially motivated, while state-sponsored cyber threat actors look to acquire large quantities of sensitive information to support broader strategic goals, such as intelligence collection. We assess that over the next two years Canadian organizations will almost certainly continue to be attractive targets for cybercriminals and state-sponsored cyber threat actors interested in obtaining personally identifiable information and other sensitive data.

Cyber threat actors have also increased the sophistication of ransomware operations by threatening to reveal confidential client information unless a ransom is paid, creating additional incentives for victims to acquiesce to their demands.[53] However, even if a payment is made, cyber threat actors can decide to delete, modify, or release information, or use stolen data in a future scam.

THE LARGEST DATA BREACH IN CANADIAN HISTORY

In October 2019, Canadian medical testing company LifeLabs was compromised by cyber threat actors, exposing the sensitive personal information of about 15 million Canadians, representing the largest single breach of personal records in Canada. The information exposed included medical test results, health card numbers, names, dates of birth, home addresses, and email addresses. While the company made a payment to retrieve the data, there is no way to be sure that the threat actors did not keep a copy of the data to further exploit or sell to other criminals.[54]

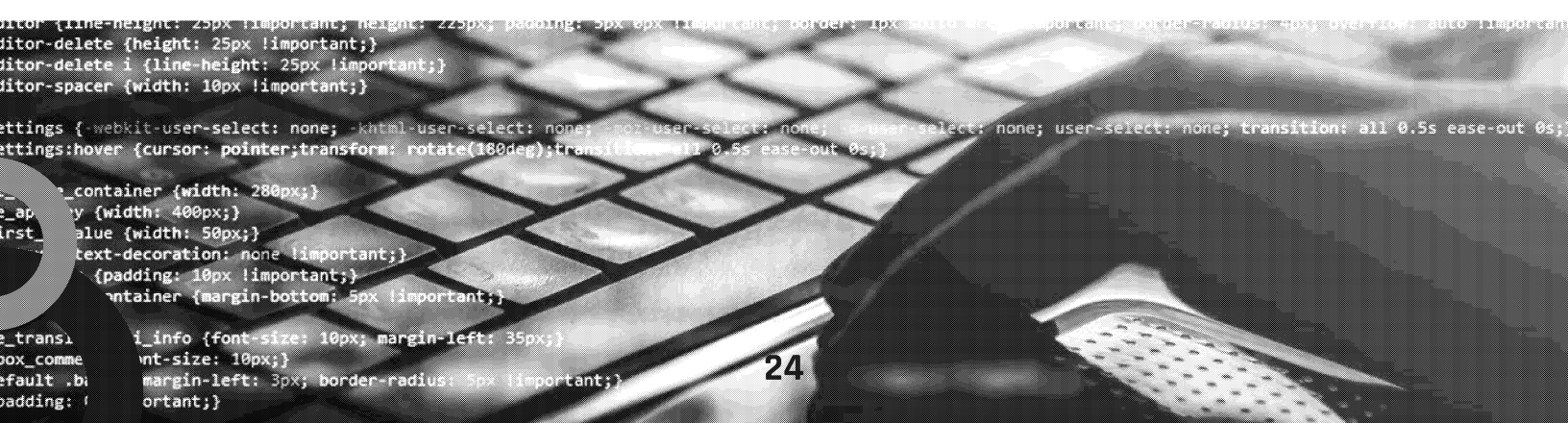
Exploiting Trusted Business Relationships

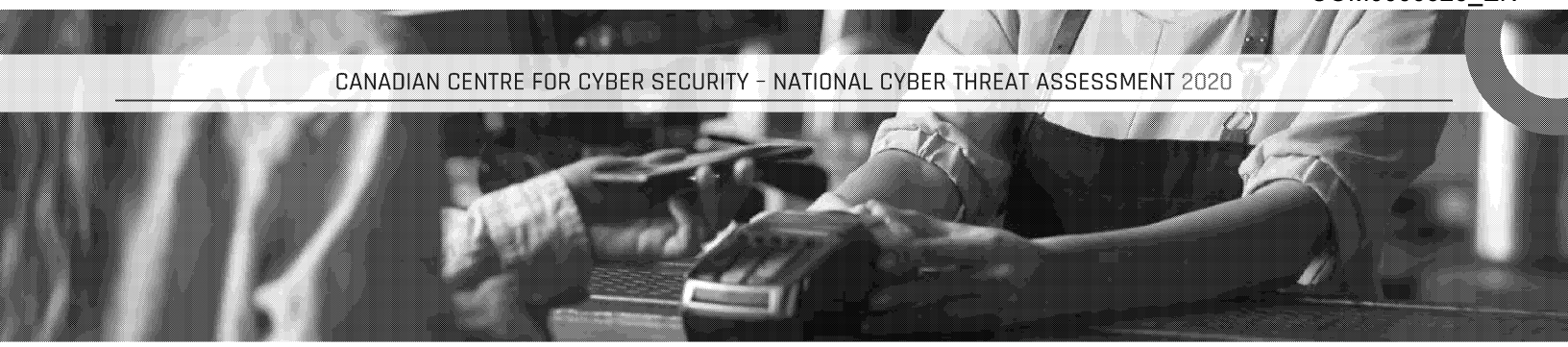
In NCTA 2018, we correctly predicted that cyber threat actors will continue to exploit the trusted relationships between businesses and their suppliers and service providers. Since 2018, financially motivated cyber threat actors have sharply increased their use of certain social engineering techniques to target organizations.[55] One of the most common and costly methods is known as business email compromise (BEC). This refers to an email designed to trick an employee in the target organization into directly transferring funds to cyber threat actors. Often, cyber threat actors impersonate high-level executives or trusted third parties. Cyber threat actors have recently been using the uncertainty surrounding the COVID-19 pandemic to target victims.

BUSINESS EMAIL COMPROMISE TARGETS MORE THAN BUSINESSES

In May 2019, a municipal government in Ontario became the victim of a BEC scam. The threat actors posed as a known and trusted city vendor. In their fake email, they requested to change the banking information for the vendor, and when this was completed, $503,000 CAD was transferred to the new account, owned by the cybercriminal.[56]

Over the past two years, cyber threat actors have expanded the use of BEC beyond traditional business victims to target religious, educational, and not-for-profit organizations.[57] We assess that cyber threat actors will very likely continue to increase their use of BECs because of their simplicity and profitability.[58] By some estimates, between 2016 and 2019, there were more than 1,200 reported cases of BEC fraud in Canada, resulting in losses of more than $45 million CAD.[59] The average BEC loss involving wire transfers is approximately $47,000 CAD.[60]





Exploiting Retail Payment Systems

Cybercriminals target payment card data by stealing credit card details and other information that victims enter on e-commerce sites, which is called formjacking.[61] In 2018, approximately 4,800 websites were victims of formjacking each month.[62] Many large websites have been compromised using this technique, including airline companies, ticket sellers, and others.[63] In 2019, more than 200 campus stores at universities and colleges in Canada and the US were affected by formjacking.[64] We assess that this trend will likely increase over the next two years as Canadians are increasingly relying on e-commerce, in part due to the COVID-19 pandemic.[65]

Cyber threat actors also continue to target point-of-sale (POS) systems used by brick-and-mortar businesses, as discussed in NCTA 2018. They do so by installing malware that can steal customer information, interfere with business operations, make fraudulent purchases, manipulate pricing, and cause other forms of disruption. In late 2019, cybercriminals targeted the POS systems at some North American gas stations to steal financial data.[66] Magnetic strip records from credit cards harvested from infected POS terminals are sold on cybercrime marketplaces and allow criminals to recreate or clone cards.

Exploiting Supply Chains

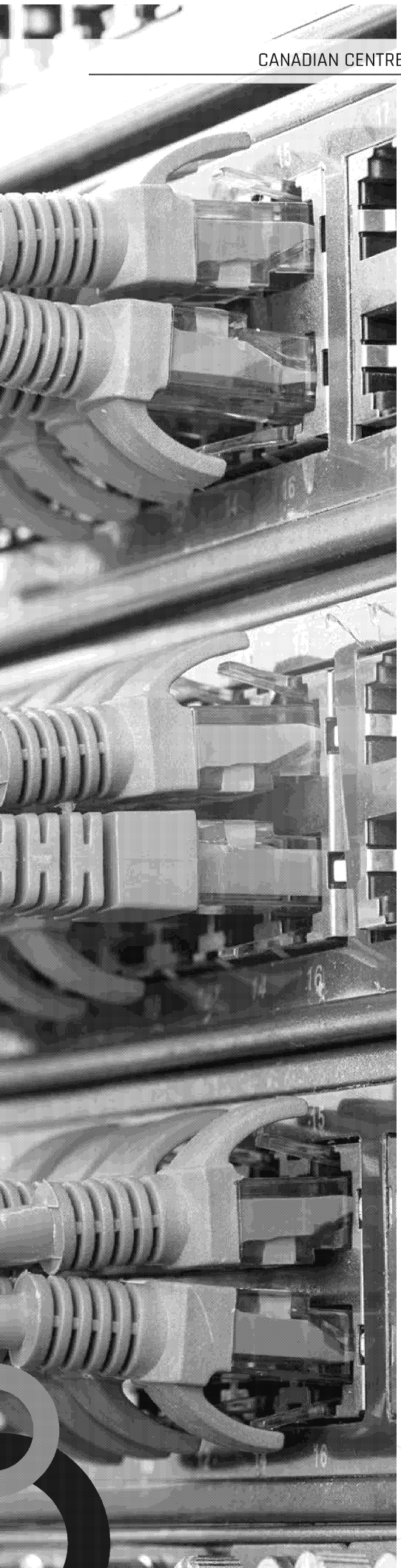
Many organizations rely on a complex and often globally distributed supply chain for many aspects of their operations, including precursor manufacturing, IT infrastructure and support, and financial services.[67] Cyber threat actors target the networks of trusted vendors and then leverage the vendors to access the networks of their true targets. Supply chain compromises can occur before or after the delivery of a product or service, or during software updates or hardware upgrades. Cyber threat actors target these updates and upgrades because they know they will be downloaded and installed thousands or millions of times in any number of organizations, and therefore create many opportunities. As Figure 6 shows, every link in a global supply chain can pose a risk to cyber security. In 2018, we correctly predicted that cyber threat actors would increasingly try to exploit supply chain vulnerabilities. We assess that cyber threat actors will almost certainly continue to exploit these vulnerabilities over the next two years.

Figure 6: Supply Chain Vulnerabilities

EXPLOITING SUPPLY CHAIN VULNERABILITIES

Since the start of the COVID-19 pandemic, cyber threat actors have gained access to a large number of hospitals globally, compromising both IT networks and ICS components and imaging products used in the healthcare industry.[68] In 2018 the same actors targeted health sector organizations in at least 24 countries, including in Canada, as well as organizations in other sectors, such as manufacturing, IT, logistics, and agriculture.[69]

We judge that it is likely that this actor compromised its victims by using software updates from trusted vendors to spread its malware.[70] We assess that the responsible actors are likely state-sponsored and interested in acquiring sensitive or proprietary information to advance national priorities.

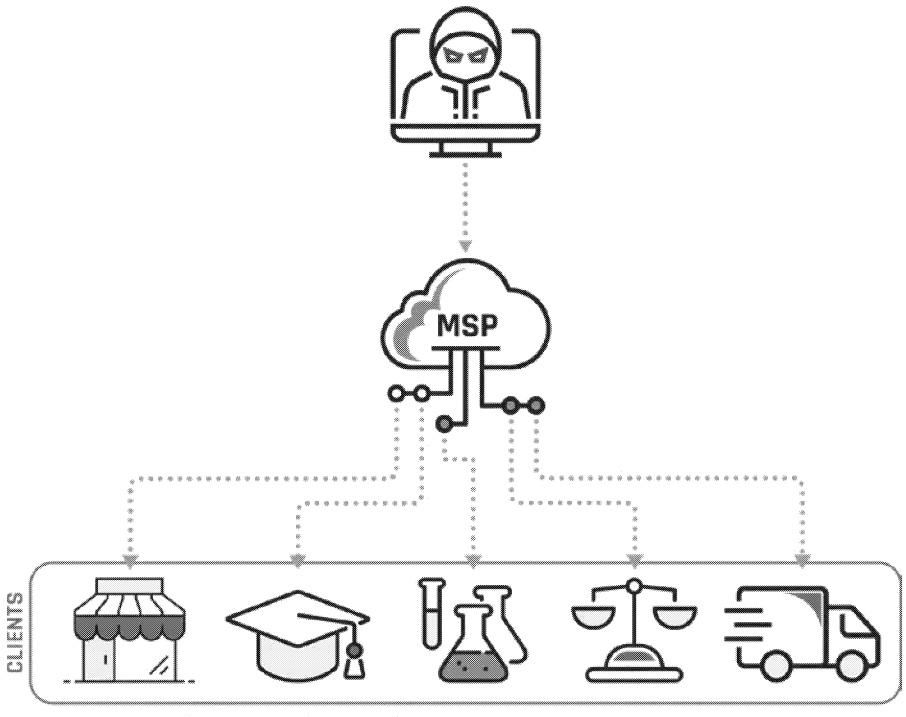


Exploiting Managed Service Providers

An MSP is a company used by organizations to provide IT services and reduce the cost of maintaining in-house IT infrastructure and personnel. When a corporate network is well-defended against direct attacks, cyber threat actors can target MSPs to obtain indirect access to client networks. In addition, threat actors who successfully compromise an MSP can reach a large number of victims: the MSP's clients.

NCTA 2018 correctly predicted that MSPs would remain attractive targets for advanced cyber threat actors. Throughout 2019, cybercriminals compromised MSPs for the purpose of abusing software used to remotely manage IT systems to automatically install ransomware on multiple client networks at once.[71] We expect that over the next two years ransomware campaigns will very likely increasingly target MSPs for the purpose of targeting their clients as a means of scaling targeted ransomware campaigns.

Figure 7: Exploitation of Managed Service Providers (MSP)



By targeting MSPs, threat actors can gain access to the MSP's clients (including businesses, universities, and other institutions) without having to compromise each client directly.

CONCLUSION

The cyber threat landscape in Canada is evolving and cyber threat actors continue to adapt their activities to keep up. In this National Cyber Threat Assessment, we identified trends within the threat landscape and the evolving cyber threat activities faced by Canadian individuals and organizations. Canadians' adoption of new technology and Internet-connected devices will usher in new threats.

As we wrote in 2018, many cyber threats can be mitigated through awareness and best practices in cyber security and business continuity. Cyber threats and influence operations continue to succeed today because they exploit deeply rooted human behaviours and social patterns, and not merely technological vulnerabilities. Defending Canada against cyber threats and related influence operations requires addressing both the technical and social elements of cyber threat activity. Cyber security investments will allow Canadians to benefit from new technologies while ensuring that we do not unduly risk our safety, privacy, economic prosperity, and national security.

The Cyber Centre is dedicated to advancing cyber security and increasing the confidence of Canadians in the systems they rely on daily, offering support to critical infrastructure networks as well as other systems of importance to Canada.

We approach security through collaboration, combining expertise from government, industry, and academia. Working together, we can increase Canada's resilience against cyber threats.

USEFUL RESOURCES

- An Introduction to the Cyber Threat Environment
- Cyber Hygiene
- Get Cyber Safe Campaign
- Spotting Malicious Email Messages
- Don't Take the Bait: Recognize and Avoid Phishing Attacks
- CRA Guidance – Protect Yourself Against Fraud
- How to Use Online Banking Securely
- How to Shop Online Safely
- Using Your Mobile Device Securely
- How Updates Secure Your Device
- Password Best Practices
- Rethink Your Password Habits to Protect Your Accounts from Hackers
- Biometrics Security
- Implementing Multi-Factor Authentication
- Password Managers Security Tips
- Using Bluetooth Technology
- Artificial Intelligence
- Joint Report on Publicly Available Hacking Tools
- Protect Your Organization from Malware
- Ransomware: How to Prevent and Recover
- Protecting Your Organization from Denial of Service Attacks
- Cyber Security Considerations for Contracting with Managed Service Providers
- Employees and Social Media
- Using Virtual Desktop At-Home and In-Office
- Virtual Private Network
- Cyber Security Tips for Remote Work
- Security Tips for Organizations with Remote Workers
- IoT Security for Small and Medium Organizations
- Supply Chain Security for Small and Medium Organizations
- Security Considerations for Research and Development
- Cyber Security for Healthcare Organizations: Protecting Yourself from Common Cyber Attacks
- COVID-19 Malicious Websites
- Focused Cyber Security Advice and Guidance during COVID-19: List of Publications by Audience
- Cyber Security Advice and Guidance for Research and Development Organizations During COVID-19
- Canadian Shield – Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic

ENDNOTES

[1] BlueLeaks Data Breach Involved 38 Canadian Police Forces." *CBC News*. 22 September 2020. https://www.cbc.ca/news/canada/ottawa/blueleaks-published-thousands-of-documents-from-canadian-police-agencies-1.5734311.

[2] "IoT Makes Industrial Manufacturers "Smart"." *PwC*. Accessed 15 July 2020. https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/iot-pov/manufacturing-iot-snapshot.html.

[3] Canada's Internet Factbook 2019." *Canadian Internet Registration Authority*. 2019. https://www.cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019. "Canadian Internet Use Survey." *Statistics Canada*. 10 May 2010. https://www150.statcan.gc.ca/n1/daily-quotidien/100510/dq100510a-eng.htm. "Canadian Internet Use Survey." *Statistics Canada* 26 November 2013. https://www150.statcan.gc.ca/n1/daily-quotidien/131126/dq131126d-eng.htm. "Canadian Internet Use Survey." *Statistics Canada*. 29 October 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm.

[4] David Vigneault. "Remarks at the Economic Club of Canada." *Government of Canada*. 04 December 2018. https://www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html.

[5] "A full year of mandatory data breach reporting: What we've learned and what businesses need to know." Office of the Privacy Commissioner of Canada." 31 October 2019. https://www.priv.gc.ca/en/blog/20191031/.

[6] "2018-19 Survey of Canadians on Privacy." *Office of the Privacy Commissioner of Canada*. 11 March 2019. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

[7] "Cyper Operations Tracker." *Council on Foreign Relations*. Accessed 15 September 2020. https://www.cfr.org/cyber-operations/.

[8] "Cybersecurity Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region – Global Forecast to 2023." *Markets and Markets*. September 2018. https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html.

[9] "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware." *US Department of the Treasury*. 05 December 2019. https://home.treasury.gov/news/press-releases/sm845; Tim Maurer. "Why the Russian Government Turns a Blind Eye to Cybercriminals." *Slate*. 02 February 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html. "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." *United States Department of Justice*. 16 September 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer; Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East." *United States Department of Justice*. 16 September 2020. https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-theft-campaign-targeting-computer-systems-united-states

[10] "Canadian Internet Governance Forum Report 2019." *Canadian Internet Registration Authority*. 27 February 2019. https://canadianigf.ca/wp-content/uploads/2019/06/2019_CIGF_report_EN-1.pdf.

[11] Hascall Sharp and Oaf Kolkman. "Discussion Paper: An Analysis of the 'New IP' Proposal to the ITU-T." *Internet Society*. 24 April 2020. https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/.

[12] Jon Fingas. "China, Huawei propose internet protocol with a built-in killswitch." *Engadget*. 30 March 2020. https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html.

[13] Craig Silverman. "How to Spot a Deepfake Like the Barack Obama - Jordan Peele Video." *Buzzfeed News*. 17 April 2018. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed.

[14] "XR Belgium posts deepfake of Belgian premier linking COVID-19 with climate crisis." *The Brussels Times*. 14 April 2020. https://www.brusselstimes.com/all-news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/.

[15] "Canadian Internet Use Survey." *Statistics Canada*. 29 October 2019. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm.

[16] Canada's Internet Factbook 2019." *Canadian Internet Registration Authority*. 2019. https://www.cira.ca/resources/corporate/factbook/canadas-internet-factbook-2019.

[17] "The Growth in Connected IoT Devices is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast." *International Data Corporation*. 18 June 2019. https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[18] Sawyer Bogdan. "Canadians have lost $43 Million to Cybercrime in 2019: OPP." *Global News*. 24 October 2019. https://globalnews.ca/news/6077016/canadians-lost-43-million-cybercrime-2019/.

[19] "Scams by Medium." *Canadian Anti-Fraud Centre*. 13 February 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-eng.htm.

[20] "Scams by Medium." *Canadian Anti-Fraud Centre*. 13 February 2020. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/medium-moyen-eng.htm.

[21] John MacFarlane. "4.2 million Desjardins members affected by data breach, credit union now says." *CBC News*. 01 November 2019. https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5344216.

[22] Aidan Wallace. "Major Data Breaches in 2019." *Toronto Sun*. 01 January 2020. https://torontosun.com/news/world/major-data-breaches-in-2019.

[23] Ken Hsu, Durgesh Sangvikar, Zhibin Zhang, and Chris Navarrete. "Lucifer: New Cryptojacking and DDoS Hybrid Malware Exploiting High and Critical Vulnerabilities to Infect Windows Devices." *Palo Alto Networks: Unit 42*. 24 June 2020. https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/.

[24] "LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario." *CBC News*. 17 December 2019. https://www.cbc.ca/news/canada/british-columbia/lifelabs-cyberattack-15-million-1.5399577.

[25] Maham Abedi. "Capital One data breach: here's what Canadians need to know." *Global News*. 30 July 2019. https://globalnews.ca/news/5702026/capital-one-data-breach-what-to-know/.

[26] Josh Fruhlinger. "Marriott data breach FAQ: How did it happen and what was the impact?" *CSO Online*. 12 February 2020. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.

[27] Roberto Rocha and Jeff Yates. "Twitter Trolls Stoked Debates About Immigrants and Pipelines in Canada, Data Shows." *CBC News*. 12 February 2019. https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

[28] Reis Thebault. "A woman's stalker used an app that allowed him to stop, start, and track her car." *The Washington Post*. 06 November 2019. https://www.washingtonpost.com/technology/2019/11/06/womans-stalker-used-an-app-that-allowed-him-stop-start-track-her-car/.

[29] "Tech Abuse and Empowerment Service." *Refuge*. Accessed 15 July 2020. https://www.refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/.

[30] "Cybersecurity Vulnerabilities Associated with Devices with Bluetooth Low Energy Chips." *Health Canada*. 11 March 2020. https://healthycanadians.gc.ca/recall-alert-rappel-avis/hc-sc/2020/72555a-eng.php.

[31] "Canada's Critical Infrastructure." *Public Safety Canada*. 19 May 2020. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx.

[32] Andy Greenberg. "The Highly Dangerous 'Triton' Hackers Have Probed the US Grid." *Wired*. 14 June 2019. https://www.wired.com/story/triton-hackers-scan-us-power-grid/.

[33] Andy Greenberg. "A Notorious Iranian Hacking Crew is Targeting Industrial Control Systems." *Wired*. 20 November 2019. https://www.wired.com/story/iran-apt33-industrial-control-systems/.

[34] "Top 2019 Cyber Attacks on ICS." *Waterfall Security*. 19 December 2019. https://waterfall-security.com/top-2019-attacks-on-ics/.

[35] Joe Tidy. "How a Ransomware Attack Cost One Firm £45m." *BBC News*. 25 June 2019. https://www.bbc.com/news/business-48661152.

[36] Andy Greenberg. "Mysterious New Ransomware Targets Industrial Control Systems." *Wired*. 03 February 2020. https://www.wired.com/story/ekans-ransomware-industrial-control-systems/; Nathan Brubaker, et. al. "Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families". *FireEye Threat Research*. 15 July 2020. https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html.

[37] "EKANS Ransomware and ICS Operations." *Dragos*. 03 February 2020. https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/.

[38] Ben Dooley and Hsako Ueno. "Honda Hackers May Have Used Tools Favored by Countries." *New York Times*. 12 June 2020. https://www.nytimes.com/2020/06/12/business/ransomware-honda-hacking-factories.html.

[39] James Lewis. "Economic Impact of Cybercrime—No Slowing Down." *Center for Strategic and International Studies and McAfee*. February 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email.

[40] "2019 Internet Security Threat Report." *Symantec*. 26 June 2019. https://www.bankinfosecurity.com/whitepapers/2019-internet-security-threat-report-w-5357.

[41] "Q1 2020 Ransomeware Marketplace Report." *Coveware*. 29 April 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[42] Ryan Flanagan. "Canadian Insurance Company Lost Nearly US$1M in Ransomware Attack." *CTV News*. 30 January 2020. https://www.ctvnews.ca/sci-tech/canadian-insurance-company-lost-nearly-us-1m-in-ransomware-attack-1.4790490.

[43] Ransomware Payments up 33% as Maze and Sodinokibi Proliferate in Q1 2020. *Coveware*. 29 April 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report.

[44] Catharine Tunney. "Ransomware Attack on Construction Company Raises Questions About Federal Contracts." *CBC News*. 26 January 2020. https://www.cbc.ca/news/politics/ransowmare-bird-construction-1.5434308; "Time's Up for Agromart Group and their Data Got Leaked by REvil Ransomware Operators." *Cyble, Inc.* 2 June 2020. https://cybleinc.com/2020/06/02/times-up-for-agromart-group-and-their-data-got-leaked-by-revil-ransomware-operators/.

[45] David Burke. "Hospitals 'Overwhelmed' by Cyberattacks Fuelled by Booming Black Market." *CBC*. 02 June 2020. https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422.

[46] "Alert: Cyber Threats to Canadian Health Organizations." *Canadian Centre for Cyber Security*. 20 March 2020. https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations.

[47] Catharine Tunney. "CSIS chief calls commercial espionage 'the greatest threat to our prosperity'." *CBC News*. 04 December 2018. https://www.cbc.ca/news/politics/david-vigneault-csis-economy-1.4932407/.

[48] "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." *US Department of Justice*. 20 December 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[49] Dustin Volz. "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets." *The Wall Street Journal*. 05 March 2019. https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800.

[50] "Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity." *Canadian Centre for Cyber Security*. 27 April 2020. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity/.

[51] "Advisory: APT29 targets COVID-19 vaccine development." *National Cyber Security Centre*. 16 July 2020. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development.

[52] "What do Cybercriminals do with the Data They Steal?" *Sysnet Global Solutions*. Accessed 10 July 2020. https://sysnetgs.com/2018/06/what-do-cybercriminals-do-with-the-data-they-steal/.

[53] Scott Ikeda. "Lifelabs Data Breach, the Largest Ever in Canada, May Cost the Company Over $1 Billion in Class-Action Lawsuit." *CPO Magazine*. 08 January 2020. https://www.cpomagazine.com/cyber-security/lifelabs-data-breach-the-largest-ever-in-canada-may-cost-the-company-over-1-billion-in-class-action-lawsuit/.

[54] Danny Palmer. "Ransomware warning: Now attacks are stealing data as well as encrypting it." *ZDNet*. 14 July 2020. https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/.

[55] "2020 Data Breach Investigations Report." *Verizon*. 02 June 2020. https://enterprise.verizon.com/resources/reports/dbir/.

[56] Bruce Sussman. "BEC Scam Costs Canadian City $500k." *SecureWorld*. 18 June 2019. https://www.secureworldexpo.com/industry-news/canada-bec-scam-example.

[57] "The Sprawling Reach of Complex Threats: 2019 Annual Security Roundup." *Trend Micro*. 25 February 2020. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats.

[58] "2019 Internet Crime Report." *Federal Bureau of Investigation*. 11 February 2020. https://pdf.ic3.gov/2019_IC3Report.pdf.

[59] C. Steven Baker. "Is That Email Really From "The Boss"? The Explosion of Business Email Compromise (BEC) Scams." *The Better Business Bureau*. September 2019. https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-explosion-of-bec-scams.pdf

[60] "Behind the 'From' Lines: Email Fraud on a Global Scale." *Agari Cyber Intelligence Division*. Accessed 15 August 2020. https://www.agari.com/insights/whitepapers/behind-the-from-lines/.

[61] "2019 Internet Security Threat Report." *Symantec*. 26 June 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[62] "2019 Internet Security Threat Report." *Symantec*. 26 June 2019. https://docs.broadcom.com/doc/istr-24-2019-en.

[63] Jin Chen, Tao Yan, Taojie Wang, and Zhanglin He. "Anatomy of FormJacking Attacks." *Palo Alto Networks, Unit 42*. 27 April 2020. https://unit42.paloaltonetworks.com/anatomy-of-formjacking-attacks/.

[64] Joseph Chen. "Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada." *Trend Micro*. 03 May 2019. https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/.

[65] Aanand Krishnan. "Web scammers are using the COVID-19 crisis to attack your customers with Magecart and other client-side exploits." *Security Boulevard*. 9 June 2020. https://securityboulevard.com/2020/06/web-scammers-are-using-the-covid-19-crisis-to-attack-your-customers-with-magecart-and-other-client-side-exploits/.

[66] Merna Emara. "Cybercrime Attacks on the Rise at North American Gas Stations, Warns Card Giant Visa." *National Post*. 17 December 2019. https://nationalpost.com/news/world/cybercrime-attacks-on-the-rise-at-north-american-gas-stations-warns-card-giant-visa.

[67] A supply chain is defined as the system of organizations, people, technology, activities, information, and resources involved in moving a product or service from a supplier to a customer. See "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." *National Institute for Standards and Technology*. April 2015. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

[68] Catalin Cimpanu. "FBI re-sends alert about supply chain attacks for the third time in three months." *ZDNet*. 31 March 2020. https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/.

[69] Howard Solomon. "Canadian Organizations Among Victims of Global Attack on Healthcare-related Industries." *IT World*. 24 April 2018. https://www.itworldcanada.com/article/canadian-organizations-among-victims-of-global-attack-on-healthcare-related-industries/404475.

[70] Johannes B. Ullrich. "Kwampirs Targeted Attacks Involving Healthcare Sector." *SANS Internet Storm Center*. 31 March 2020. https://isc.sans.edu/forums/diary/Kwampirs+Targeted+Attacks+Involving+Healthcare+Sector/25968/?utm_medium=Social&utm_source=Twitter&utm_campaign=SANS+Central.

[71] Catalin Cimpanu. "GandCrab Ransomware Gang Infects Customers of Remote IT Support Firms." *ZDNet*. 14 February 2019. https://www.zdnet.com/article/gandcrab-ransomware-gang-infects-customers-of-remote-it-support-firms/; Catalin Cimpanu. "Ransomware Gang Hacks MSPs to Deploy Ransomware on Customer Systems." *ZDNet*. 20 June 2019. https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/; Catalin Cimpanu. "Ransomware Hits Hundreds of Dentist Offices in the US." *ZDNet*. 29 August 2019. https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.