



CANADIAN CENTRE FOR
CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT 2018



Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada 

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

ABOUT THE CYBER CENTRE

Launched on 1 October 2018 as part of the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (Cyber Centre) is a new organization but one with a rich history. The Cyber Centre brings operational security experts from across the Government of Canada under one roof. In line with the *National Cyber Security Strategy*, the launch of 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.

Developing and sharing our **specialized cyber defence technology and knowledge**, helping to improve cyber security for all Canadians.

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](https://cyber.gc.ca),
OR FOLLOW US ON TWITTER [@CYBERCENTRE_CA](https://twitter.com/cybercentre_ca)**

FOREWORD

The Canadian Centre for Cyber Security (Cyber Centre) is the Government of Canada's authority on cyber security. As part of the Communications Security Establishment (CSE), the Cyber Centre brings over 70 years of experience protecting Canada's most sensitive information and networks. In line with the June 2018 National Cyber Security Strategy, the Cyber Centre was created to be a source of trusted, expert cyber security advice and guidance for government, industry partners such as critical infrastructure owners and operators, and for the Canadian public.

This National Cyber Threat Assessment describes our view of the current cyber threat environment facing Canada and Canadians. The intent of this assessment is to ensure that as cyber threat actors pursue new ways to use the Internet and connected devices for malicious purposes, Canadians are well informed of the cyber threats facing our country. You will note that we do not name those affected by cyber compromises. This is deliberate. In this assessment we focus on analyzing cyber threat actors and their activities.

Canada is one of the most connected countries in the world. A safe and secure cyber space is important for Canada's security, stability, and prosperity. The interconnected nature of the threats highlighted in this assessment demonstrates that effective cyber security requires collaboration. The Cyber Centre works closely with government, industry partners, and the public to share our unique knowledge and experience to improve the cyber security of Canada and all Canadians. We must all work together to make Canada safer online.

It is certain that Canadians will be affected by malicious online activity in the coming year, but by knowing the threats, we hope that action can be taken to prevent, detect, and respond.

Although cyber threats to Canada and Canadians are serious, I am confident that by working together we can make our country more resilient against cyber threats.

Scott Jones
Head, Canadian Centre for Cyber Security

www.cyber.gc.ca

EXECUTIVE SUMMARY

In our highly connected digital society, Canadians and Canadian organizations rely on the Internet for both personal and professional activities. It is in this context that we assess cyber threats to Canadian individuals, businesses, and critical infrastructure, including government.

Cyber threat activity against Canadians often has financial or privacy implications. Yet cyber threat activity against Canadian businesses and critical infrastructure can have more far-reaching consequences, such as operational disruptions to the financial sector, large-scale theft of personal information, and even potential damage to infrastructure.

KEY JUDGEMENTS

- Cybercrime is the cyber threat most likely to affect Canadians and Canadian businesses in 2019.** Cybercrime is evolving as cybercriminals take advantage of growing online markets for illicit goods and services in order to maximize their profits. Cybercriminals tend to be opportunistic when looking for targets, exploiting both technical vulnerabilities and human error.
- Cyber threat actors – of all sophistication levels – will increase the scale of their activities to steal large amounts of personal and commercial data.** Data, such as intellectual property and Canadians' personal information, are used for theft and resale, fraud, extortion, or espionage.
- Canadians are very likely to encounter malicious online influence activity in 2019.** In the coming year, we anticipate state-sponsored cyber threat actors will attempt to advance their national strategic objectives by targeting Canadians' opinions through malicious online influence activity.
- State-sponsored cyber threat actors will continue to conduct cyber espionage against Canadian businesses and critical infrastructure to advance their national strategic objectives.** More nation-states are developing cyber tools designed to conduct cyber espionage.
- It is very unlikely that, absent international hostilities, state-sponsored cyber threat actors would intentionally disrupt Canadian critical infrastructure.** However, we also assess that as all manners of critical infrastructure providers connect more devices to the Internet, they become increasingly susceptible to less-sophisticated cyber threat actors, such as cybercriminals.
- Sophisticated cyber threat actors will likely continue to exploit the trusted relationships between businesses and their suppliers and service providers for espionage and cybercrime purposes.**
- Cyber threat actors are adopting more advanced methods, such as compromising hardware and software supply chains, making detection and attribution more difficult.**

Adopting even basic cyber security practices can help thwart cyber threat actors and reduce the threats to Canadians and Canadian businesses.

TABLE OF CONTENTS

ABOUT THIS DOCUMENT	7
EFFECTS OF CYBER THREAT ACTIVITY	8
CYBER THREATS TO CANADIANS	10
Cybercrime	11
Malicious Online Influence Activity	14
CYBER THREATS TO CANADIAN BUSINESSES	16
Data Breaches	18
Exploiting Trusted Relationships	19
CYBER THREATS TO CANADIAN CRITICAL INFRASTRUCTURE	22
Increasing Cyber Threat Exposure	24
Public Institutions and Sensitive Information	26
CONCLUSION	27
USEFUL RESOURCES	28
ENDNOTES	29

ABOUT THIS DOCUMENT

This document highlights the cyber threats facing individuals, businesses, and critical infrastructure in Canada. We recommend reading this assessment along with the [Introduction to the Cyber Threat Environment](#). 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 [Top 10 IT Security Actions](#) and 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.

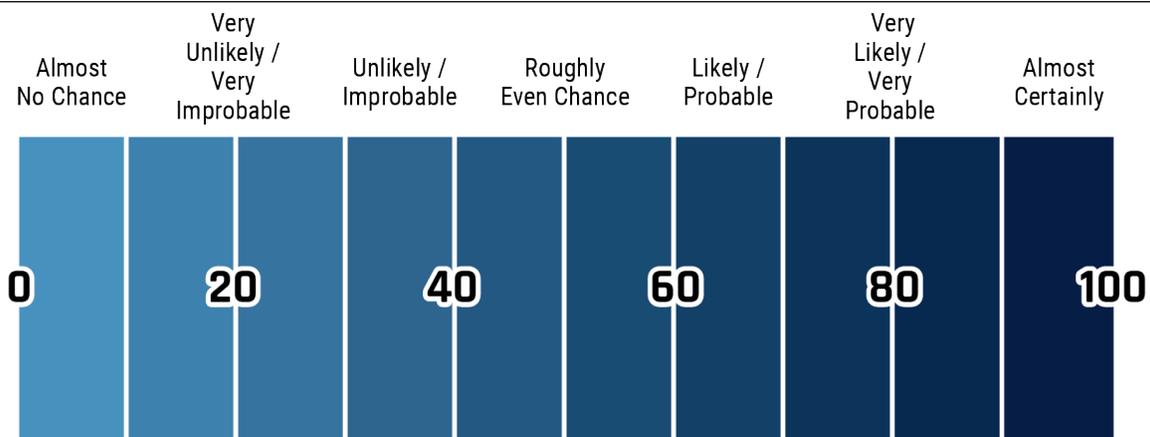


ASSESSMENT PROCESS

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 15 October 2018.

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.





EFFECTS OF CYBER THREAT ACTIVITY

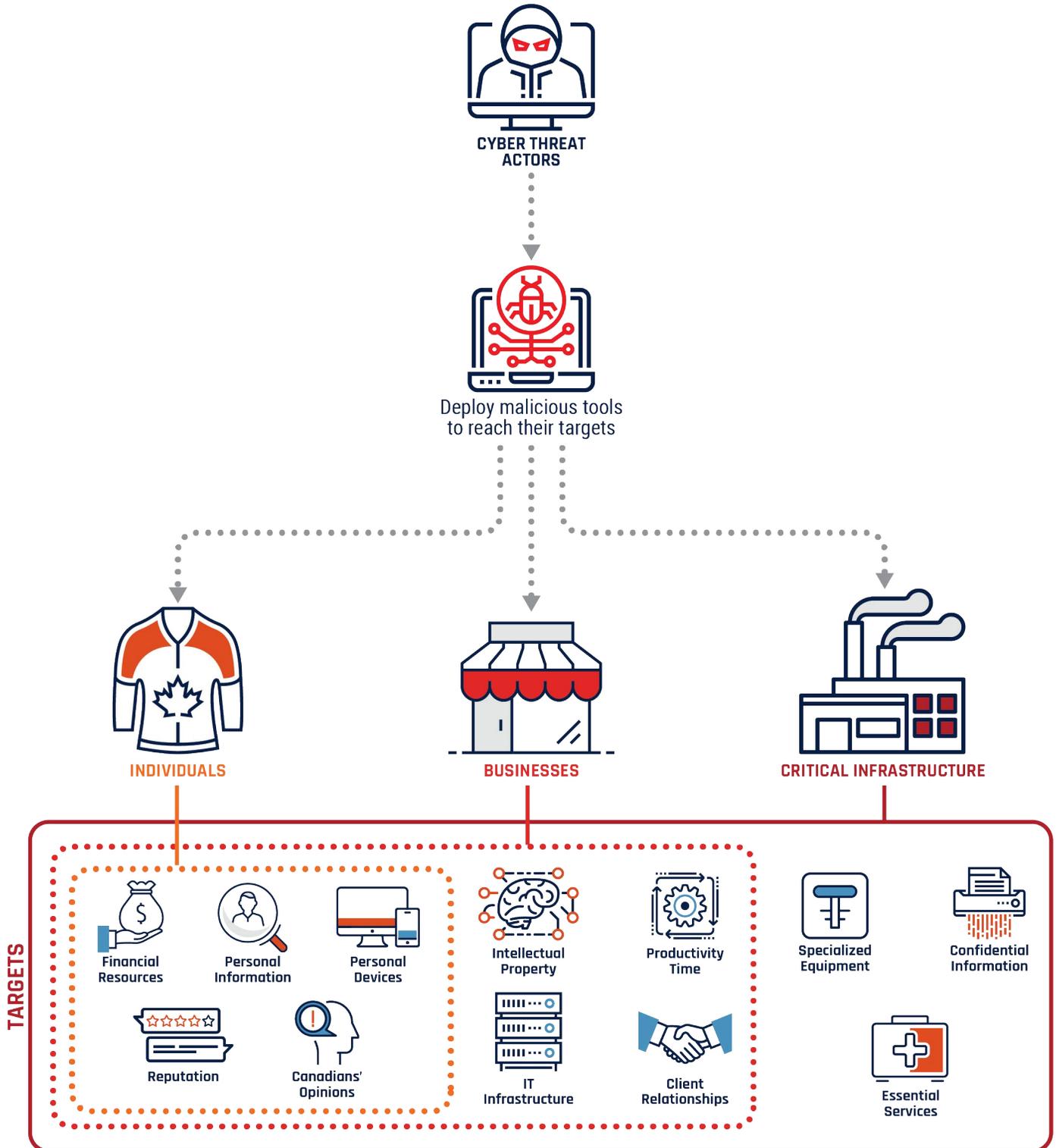
Canadians and Canadian organizations are connecting more of what they value most to the Internet. Malicious cyber threat actors – many of whom operate outside our borders – take advantage of security gaps, low cyber security awareness, and new technological developments as they try to compromise cyber systems. In this assessment, we look at cyber threat activity according to how it can affect Canadian individuals, businesses, and critical infrastructure.¹

Cyber threat actors target anything connected to, or residing on, the Internet including:

- **Technology**, such as personal devices and industrial equipment;
- **Information**, such as intellectual property and personal and confidential details;
- **Resources**, such as financial assets and productivity;
- **Relationships**, such as supply chains and essential services; and
- Our **opinions** and **reputations**.

Figure 1: Cyber threat actor targeting

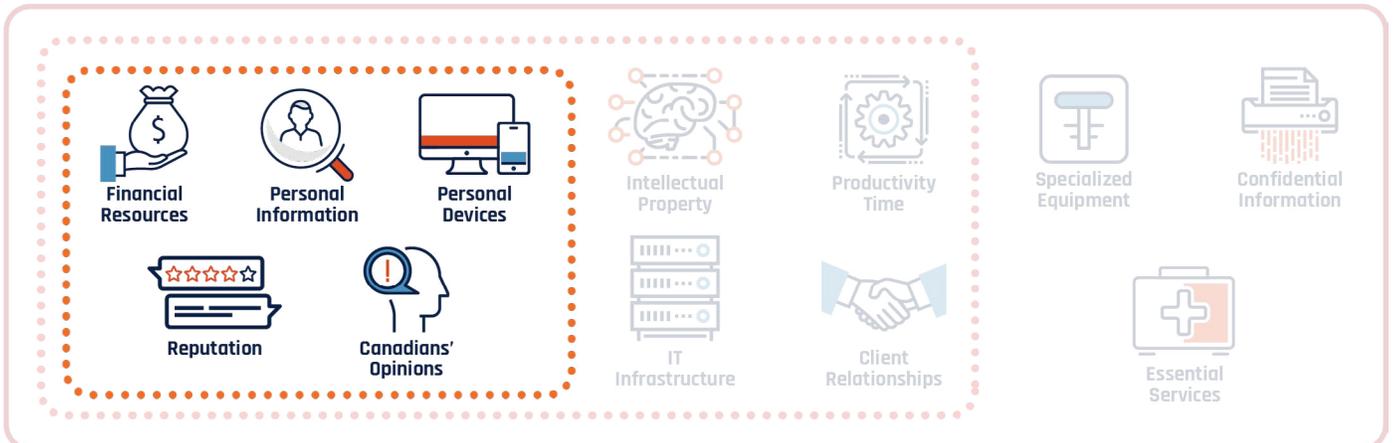
Cyber threat actors deploy a variety of malicious tools to reach their targets. Some types of targets, such as financial and banking information or personal information, are held by individuals and organizations alike. Some systems that cyber threat actors target, such as government networks used to maintain essential services, are held by critical infrastructure providers.





CYBER THREATS TO CANADIANS

TARGETS



CYBERCRIME

As Canadians put more of their information online, they become increasingly attractive targets for cyber threat actors. With cybercriminals continuing to adapt and improve their cyber capabilities to steal, commit fraud, or extort money from Canadians, we assess that cybercrime is the cyber threat Canadians and Canadian organizations are most likely to encounter.²

Stealing Personal and Financial Information

Stealing personal and financial information is lucrative for cybercriminals and is very likely to increase. Cybercriminals profit at the expense of Canadians by obtaining account login credentials, credit card details, and other personal information. They exploit this information to directly steal money, to resell information on cybercrime marketplaces, to commit fraud, or for extortion. Increasingly, we see cybercriminals becoming more organized, developing business-like processes to expand their operations to take advantage of vulnerabilities in software, hardware, and human behaviour online. For example, in recent years, cybercriminals have designed **banking trojans** specifically for mobile phones to steal user data and target financial resources.

Cybercrime is now so prevalent and sophisticated that it sustains illegal online marketplaces. These cybercrime marketplaces offer illicit goods, stolen information, and **malware**. Some cybercrime marketplaces even offer customer support and rating functions. More accessible and easy-to-use cyber tools help cybercrime proliferate and operate around the world, often in areas beyond the reach of Canadian law enforcement agencies.

Increasing Cyber Threat Exposure

Canadians' exposure to cyber threats increases with the growing number of Internet-connected devices, such as televisions, home appliances, thermostats, and cars. Manufacturers have rushed to connect more types of devices to the Internet, often prioritizing ease of use over security. We regularly observe cyber threat actors exploiting security flaws in devices resulting in either disruption to device functionality or using devices as platforms to launch other malicious cyber activities.

We have also observed malware used to find system vulnerabilities, allowing cyber threat actors to carry out unauthorized activity, such as launching a **botnet**. In fact, we judge that cyber threat actors are likely shifting their preferred platform for botnets from personal computers to other Internet-connected devices.



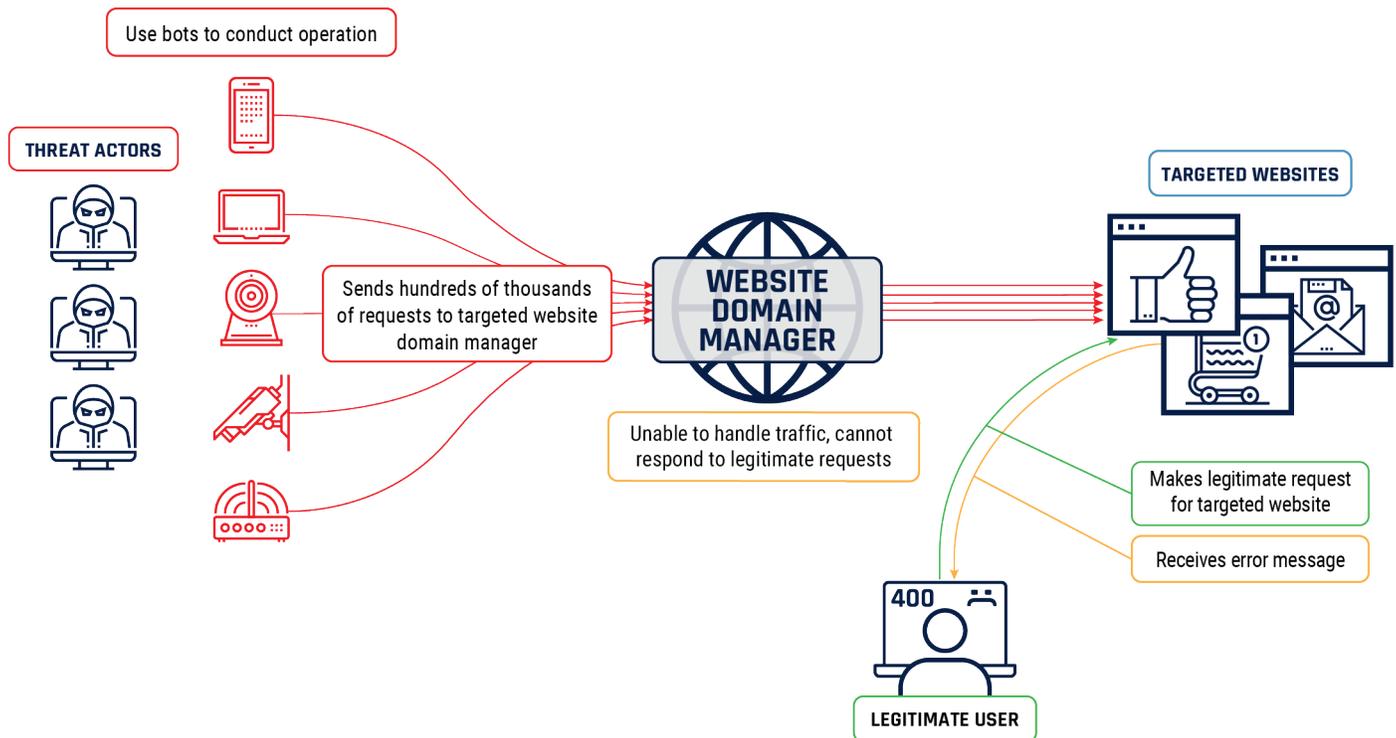


DOMAIN NAME SYSTEM PROVIDER DISRUPTION

In October 2016, cybercriminals used a botnet made up of thousands of poorly secured Internet-connected devices in an attempt to artificially generate advertising revenue online. The compromised devices included routers, air quality monitors, baby monitors, surveillance cameras, and other equipment using default usernames and passwords. The botnet conducted a powerful Distributed Denial of Service that disrupted a major website domain manager, temporarily disabling some of the world's most popular e-commerce, entertainment, and social media sites for millions of users. One of the cybercriminals posted this malware on a cybercrime forum, which let other cyber threat actors create variants of the botnet to use for other malicious activities.³

The case demonstrates how cybercriminals can exploit a variety of devices to conduct high-profile operations and also advertise their capabilities. By sharing and modifying malware source code, cybercriminals attempt to mask their identities in an effort to avoid legal consequences.

Figure 2: Distributed denial of service



Financing Criminal Enterprise

Connecting more and more devices to the Internet has also created opportunities for cybercriminals to use malware to generate or "mine" cryptocurrency. In order to do this, cybercriminals use malware that takes control of a device's processing power for their own purposes, interfering with a device's functionality. Depending on the type of malware, affected users may not notice anything unusual about their device, while others may experience slower performance, a rapidly drained battery, increased data charges, or a shortened device lifetime.⁴ We expect that cybercriminals will continue to develop malware to conduct unauthorized cryptocurrency mining in 2019, especially if cryptocurrency values rise.

Figure 3: Ransomware



Fraud and Extortion

We have observed increasing sophistication in the types of cyber fraud and extortion attempts directed at Canadians. We expect this trend to continue as cybercriminals acquire new tools. Cyber threat actors conduct fraud by posing as legitimate organizations, such as government institutions, banks, or law firms in order to trick Canadians into clicking on malicious links or attachments that attempt to download malware onto their devices. We have also observed cyber threat actors posing as trusted software providers using pop-up ads to lure unsuspecting users into downloading malware.



FAKE CANADA REVENUE AGENCY MESSAGE

Cyber threat actors posing as the Canada Revenue Agency (CRA) have sent fraudulent emails and text messages to Canadians requesting personal information, such as their social insurance number, credit card information, or passport number. Some scams allege that personal information is required so a taxpayer can receive a refund; others threaten that recipients must pay a bogus debt.⁵

Scams such as these are a reminder that it is not hard for cyber threat actors to find or develop content resembling a legitimate, trusted source. Phishing messages designed to appear legitimate are a simple, common, and often very effective form of compromise. Links and documents attached to these messages are likely malicious, containing banking trojans or other malware that cyber threat actors use to steal Canadians' money or identities.

Cybercriminals use both cyber tools and social engineering to extort money or information from Canadians.⁶ The most common form of malware used for extortion is **ransomware**. After cybercriminals infect a device with ransomware, they try to extort money from owners by encrypting their data. Ransomware is no longer a sophisticated cyber tool. Low-sophistication cyber threat actors can now access it as a service that they rent or purchase on cybercrime marketplaces.



EXTORTION SCAM AND THE CYBERCRIME MARKETPLACE

In summer 2018, some Canadians reported receiving a message threatening to release a compromising video of them, allegedly recorded as they viewed pornography. The cyber threat actors included a password in their messages that they presented as proof they had compromised recipients' devices. The cyber threat actors then demanded a bitcoin transfer or they would send the video to a recipient's contacts. In reality, no compromise of the user devices had occurred and the cyber threat actors had not recorded any videos. Individuals who did not pay the extortion fee received no further messages.⁷

The scam shows how cybercriminals provide services for one another. The passwords used in this scam very likely came from one of many unrelated data breaches involving theft of login credentials from a website. A cybercriminal likely made the login credentials available for sale on a cybercrime marketplace. Another cybercriminal could have then bought these email addresses and passwords and sent the threatening messages. This type of scam appeals to common fears such as violation of privacy and embarrassment.

MALICIOUS ONLINE INFLUENCE ACTIVITY

In addition to cybercrime, cyber threat actors also try to manipulate our opinions. Many web platforms, including social media, use legitimate tools created for advertising and information-sharing to connect users to content and products. However, state-sponsored cyber threat actors try to exploit these legitimate tools to conduct malicious online influence activity and advance their national strategic objectives. We assess that in 2019, state-sponsored cyber threat actors will very likely attempt to advance their national strategic objectives by targeting Canadians' opinions through malicious online influence activity.

State-sponsored cyber threat actors can conduct sophisticated online influence operations by posing as legitimate users. They create social media accounts or hijack existing profiles to promote content for the purpose of manipulating individuals. They establish "troll farms" consisting of employees paid to comment and share content on traditional media websites, social media, and anywhere else they can reach their target audience. Cyber threat actors also try to steal and release information, modify or make information more compelling and distracting, create fraudulent or distorted "news," and promote extreme opinions.⁸

Cyber threat actors can also amplify – or suppress – social media content using botnets, which automate online interactions and share content with unsuspecting users. Botnets share memes, promote hashtags, and harass legitimate users to create the impression that hundreds, thousands, or even millions of people share a cyber threat actor’s views. By spreading their preferred content among large numbers of paid and legitimate users, cyber threat actors can promote their specific point of view and potentially influence Canadians. Although major web platforms are making efforts to curb the negative effects of manipulative information sharing, the opinions of Canadians will remain an attractive target for cyber threat actors seeking to influence Canada’s democratic processes.

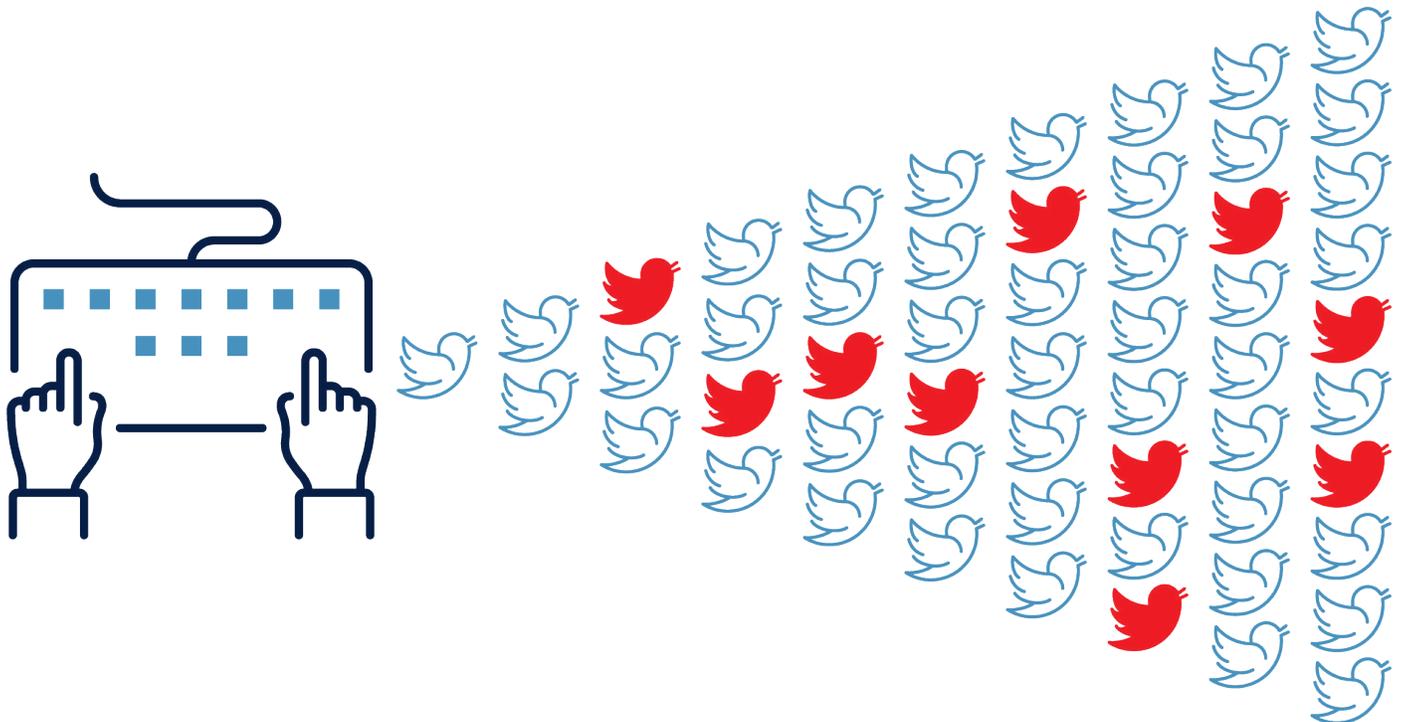
State-sponsored cyber threat actors seeking to influence democratic processes are also capable of conducting activity against organizations involved in elections, as well as politicians, political parties, and traditional media outlets. For more analysis, see the Communications Security Establishment’s [“Cyber Threats to Canada’s Democratic Process”](#) (2017).



RUSSIAN TROLLS STIR CANADIAN ISSUES

A recent study revealed Twitter accounts connected to the Russian-based Internet Research Agency that promoted divisive and inflammatory content before the 2016 United States presidential election also tweeted about events in Canada. About 8,000 of over 3 million archived tweets from the now-deleted accounts focused on Canadian issues, including the May 2016 fire in Fort McMurray, the January 2017 Québec City mosque shooting, and the increase in asylum-seeker border crossings in summer 2017. The Russian trolls attempted to create confusion by inserting false information into online discussions and exacerbating existing differences of opinion.⁹ This case demonstrates that Canadian social media users can be exposed to foreign malicious influence activity.

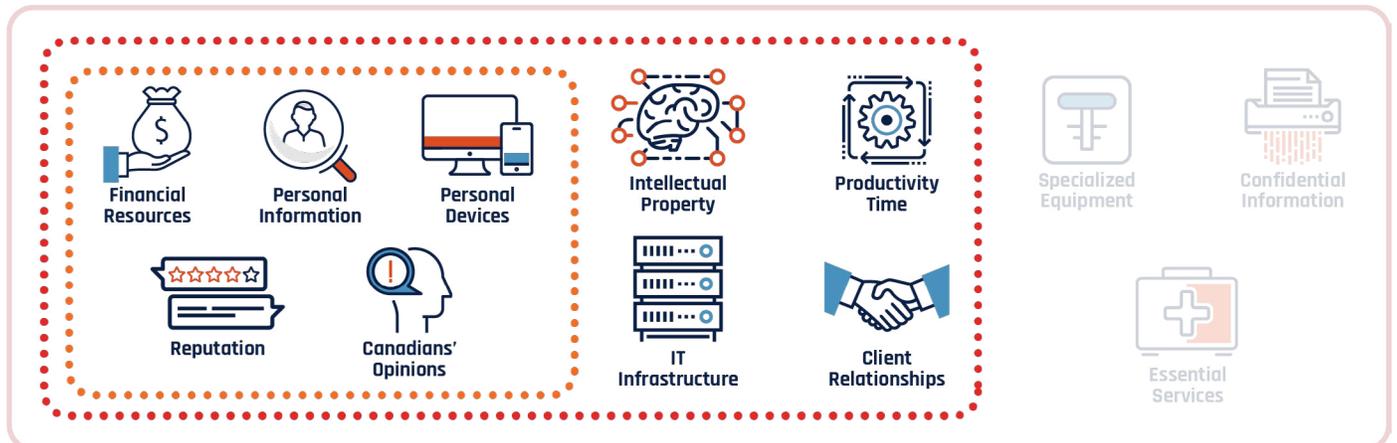
Figure 4: Cyber threat actors post misleading and false content





CYBER THREATS TO CANADIAN BUSINESSES

TARGETS



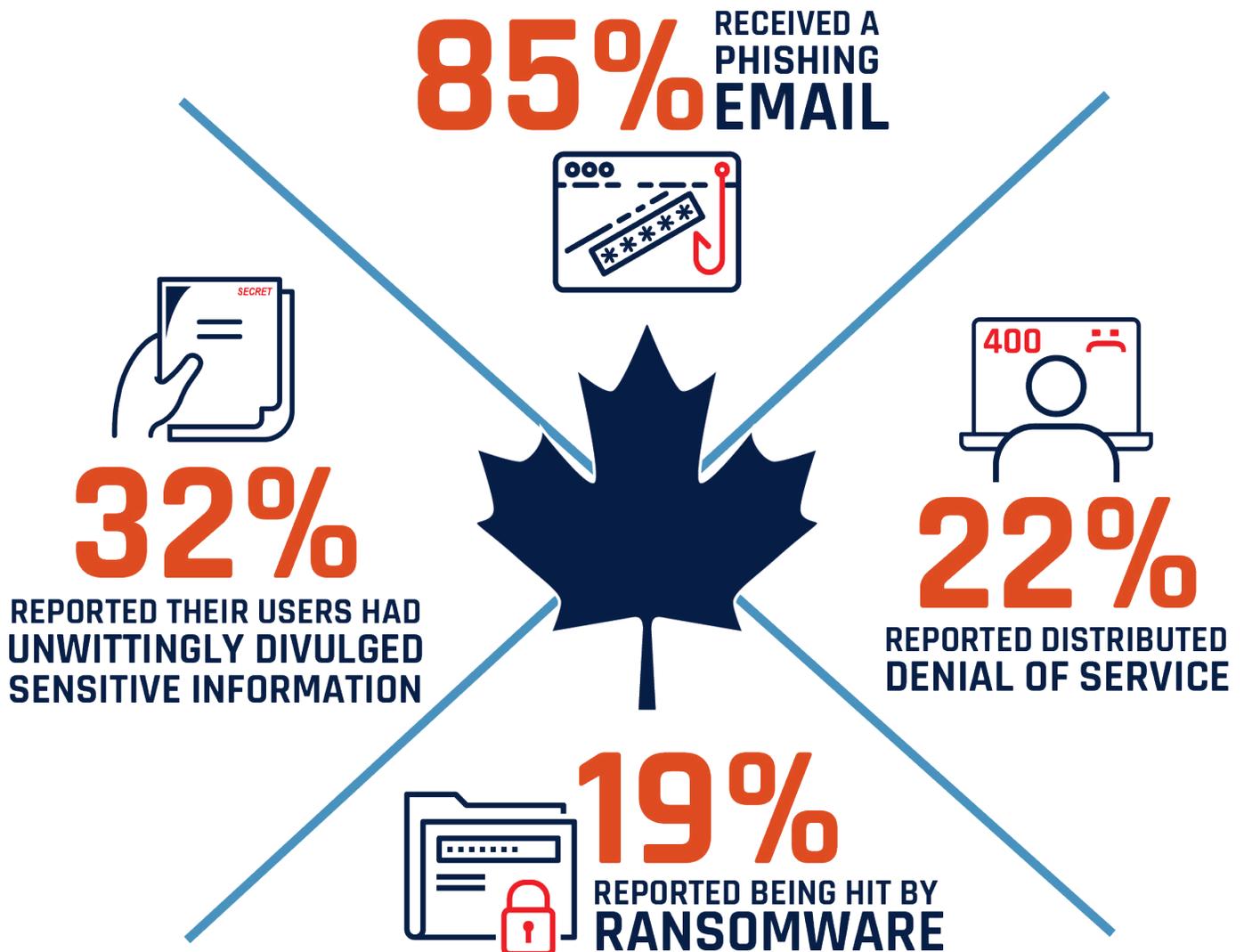
We assess that cybercriminals are – and will continue to be – the greatest cyber threat facing businesses of all sizes in 2019. Cyber threat actors target Canadian businesses for their data about customers, partners and suppliers, financial information and payment systems, and proprietary information.

Stolen information is often held for ransom, sold, or used to gain a competitive advantage. Beyond financial losses from theft or ransom payments, cyber incidents can also result in reputational damage, productivity loss, intellectual property theft, operational disruptions, and recovery expenses.

Targeting Business Executives

Cyber threat actors use specific social engineering techniques against businesses. An increasingly common method is known as **whaling**. This term refers to spear-phishing aimed specifically at senior executives or other high profile recipients with privileged access to company resources. Whaling occurs when an executive with authority to issue large payments receives a message appearing to come from a relevant department or employee, urging them to direct funds to an account controlled by a cyber threat actor. This type of social engineering can lead to major financial losses and reputational damage, but it also requires internal information that is often difficult to obtain. Like other social engineering techniques, whaling is designed to exploit predictable human behaviour.

Figure 5: Canadian Internet Registration Authority Survey 2017-2018¹⁰
In a survey of 1,985 Canadians who owned a ".ca" domain between November 2017 and January 2018, including personal and business websites



Exploiting Retail Technology

Cyber threat actors also target point-of-sale systems used in the retail and hospitality sectors. By targeting out-of-date IT systems, cyber threat actors can install malware that steals customer information, interferes with business operations, makes fraudulent purchases, manipulates pricing, and causes other forms of disruption.

Although prices vary, stolen credit card numbers on cybercrime marketplaces sell for minimal amounts. Cybercriminals can package credit card numbers with personal details about card holders such as their addresses and mothers' maiden names. Cybercrime marketplaces also offer magnetic strip records from credit cards that allow criminals to recreate cards. Similar to legal markets, sellers offer discounts for bulk purchases.

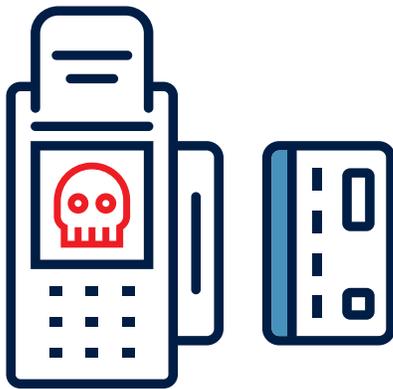
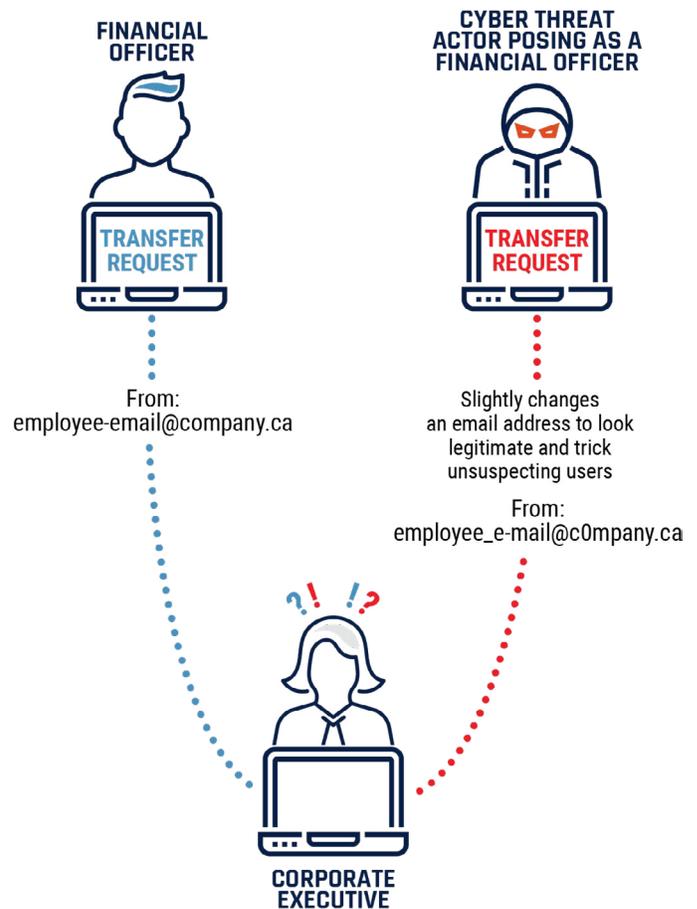


Figure 6: Whaling



DATA BREACHES

Stealing Customer and Client Data

Cyber threat actors have both the intent and capability to acquire sensitive information as demonstrated by numerous high-profile data breaches targeting the data of millions of customers around the world. Large databases containing personal information such as names, addresses, phone numbers, financial details, and employment information are valuable to cyber threat actors. The aggregation of data collected from multiple breaches can provide cyber threat actors the ability to build comprehensive profiles to conduct cyber threat activity against specific groups or individuals.

We assess that in 2019 large databases will almost certainly remain attractive targets for cyber threat actors seeking to sell information or support state-sponsored espionage.

Cyber threat actors also attempt to extort businesses by threatening to reveal confidential client information. Some businesses decide that paying a ransom is cheaper than the costs associated with ignoring a cyber ransom. Yet, cyber threat actors can decide to delete, modify, or release information, even if a payment is made. Robust cyber security and business continuity practices are required to protect valued data.



PROJECT ADORATION

In January 2017, the Royal Canadian Mounted Police (RCMP) took down a website hosting 3 billion personal records collected from major global data breaches. Although the RCMP located the servers hosting personal content in Canada, users from around the world could access the information for a small fee. In December 2017, the RCMP charged an individual alleged to have trafficked identity information.¹¹

This case is a revealing example of how cybercriminals profit by using personal information stolen from data breaches. While cybercriminals exploit the transnational nature of the Internet, operations such as Project Adoration, which involved cooperation between the RCMP, the Dutch National Police, and the United States Federal Bureau of Investigation, demonstrate that law enforcement is advancing systems and methods to tackle cybercrime. This case highlights the importance of international partnerships to investigate and prosecute cybercriminals.



EXTORTION BY CUSTOMER DATA

In May 2018, cybercriminals contacted two Canadian banks, claiming to have accessed the personal information of tens of thousands of clients. The cybercriminals threatened to release the information unless the banks paid them \$1 million ransom. Both banks refused to pay, offered clients free credit monitoring, and pledged to cover any money lost from affected bank accounts due to fraud.¹²

This case shows that a business's commitment to maintaining client confidentiality can be exploited in an attempt to extract payment. A similar operation against a business with fewer resources could inflict devastating damage by extorting funds that disable operations or releasing information and damaging its reputation.

Commercial Espionage

Canadian businesses, especially those active in strategic sectors of the economy, are subject to cyber espionage aimed at stealing intellectual property and other commercially sensitive information. Cyber threat actors target commercial information so they can copy existing products, undercut competition, or gain an advantage in business negotiations. Generally, commercial espionage requires advanced capabilities and a persistent approach.

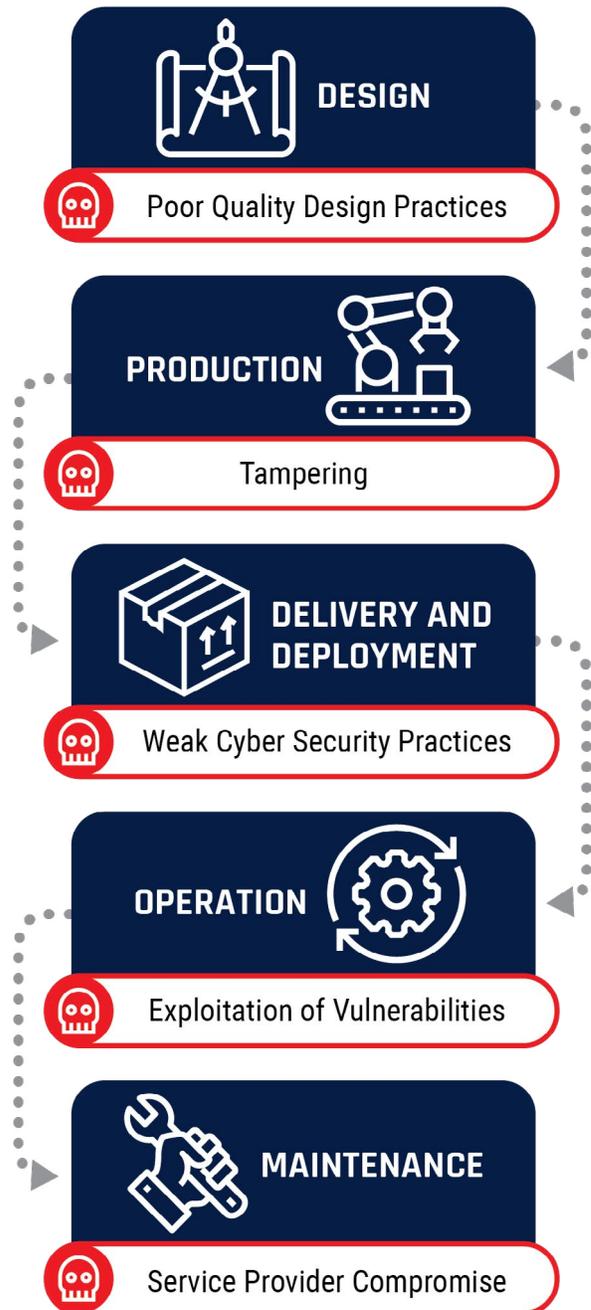
We have observed some adversarial nation-states advance their defence and technology sectors by conducting cyber commercial espionage around the world, including in Canada. This cyber threat activity can harm Canada's competitive business advantage and undermine our strategic position in global markets.

We assess that the threat of cyber espionage is higher for Canadian businesses when they operate abroad. Many countries have the legal and technological framework that enables their domestic police or security forces to covertly access data when it transits or resides in their country. Canadian businesses operating abroad should remain mindful of local laws, regulations, and business practices, and the threats these may present to their proprietary information, personal data, or intellectual property.

EXPLOITING TRUSTED RELATIONSHIPS

We assess that sophisticated cyber threat actors will likely continue to exploit the trusted relationships between businesses and their suppliers and service providers. Cyber threat actors can gain access to a business's network by exploiting the equipment of a supplier prior to product delivery or by compromising a service provider's connections to a partner or client.

Figure 7: Supply Chain Process¹³





SOFTWARE UPDATE COMPROMISE

In September 2017, malware in a software update for a program designed to improve device performance, allowed cyber threat actors to bypass a device's authentication and encryption. The malware affected 2.2 million users around the world. According to media reports, cyber threat actors targeted the data and intellectual property of 18 companies for espionage purposes, including major global technology manufacturers.¹⁵

This case illustrates how trusted software can become a vehicle for cyber threat actors seeking to compromise devices and access proprietary data owned by technology manufacturers. It also shows how millions of devices can become infected in a malicious campaign, even if they are not the intended targets. Compromising many devices disguises a cyber threat actor's motivations, making attribution more difficult.

Supply Chain Compromises

Many businesses rely on a complex, often globally distributed, supply chain that consists of many levels of component suppliers and developers.¹⁴ It is likely that cyber threat actors will increasingly try to exploit supply chain vulnerabilities because security improvements have made devices and the information they contain more difficult to target directly.

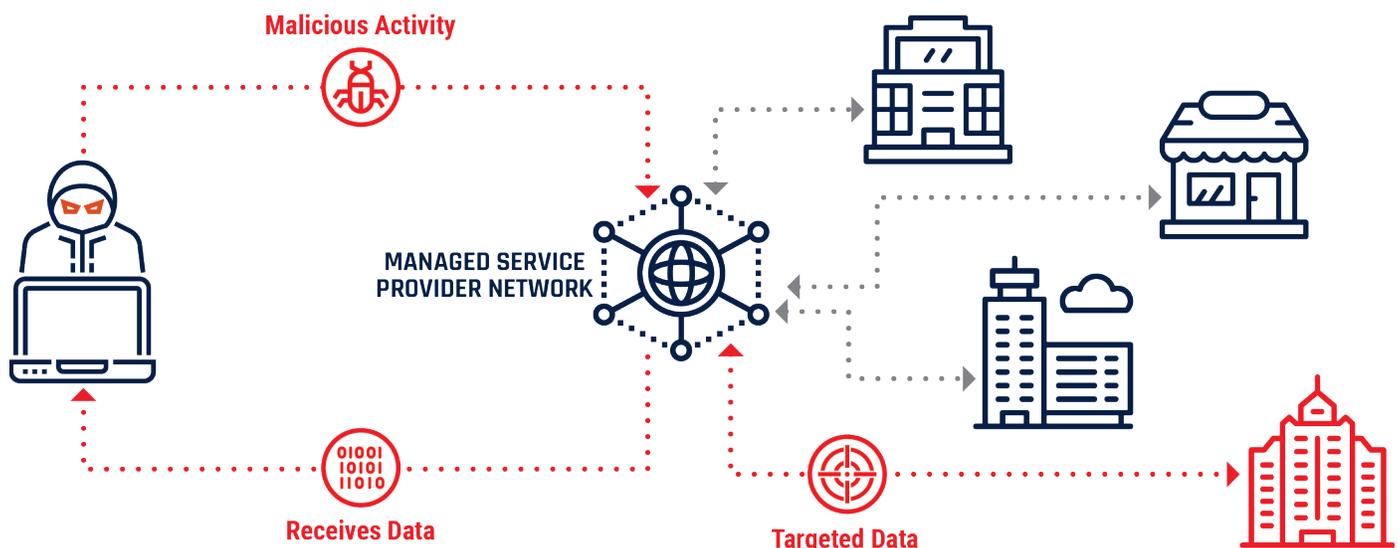
Given the interdependent nature of many modern businesses, supply chain security is only as strong as its weakest link. As Figure 7 on the previous page shows, every link in a global supply chain can pose a threat to cyber security. A supply chain compromise allows cyber threat actors to exploit a device, or one of its components, even before the device is connected to a business's secured network. Supply chain compromises can occur before or after the delivery of a product or service, or during software updates or hardware upgrades.

Managed Service Providers

We assess that in 2019 cyber threat actors will likely continue exploiting relationships of trust by identifying vulnerable parties and accessing shared networks to reach their primary target.

A **managed service provider (MSP)** is a company used by businesses to provide IT services and reduce the cost of maintaining in-house IT personnel. To be effective, MSPs typically have extensive access to a client's network. MSPs that have many clients become a connection point among many networks. When cyber threat actors compromise a major MSP, they can obtain access to some or all of its clients' networks and their digital property. We assess it is very likely that MSPs will remain attractive targets for advanced cyber threat actors because of their privileged connections to businesses' networks and information.

Figure 8: MSP targeting



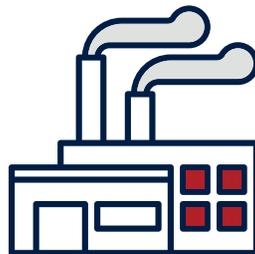


STRATEGIC MSP COMPROMISE

In April 2017, cyber security researchers uncovered a major cyber espionage campaign targeting global MSPs. By exploiting the network connections between MSPs and their clients, the cyber threat actors moved from a small number of initially compromised MSPs to the networks of thousands of clients, including some in Canada. The cyber threat actors stole intellectual property and sensitive data from MSPs and their clients in sectors including engineering and construction, retail, industrial manufacturing, energy and mining, precious metals, technology, pharmaceuticals and life science, and business and professional services.¹⁶

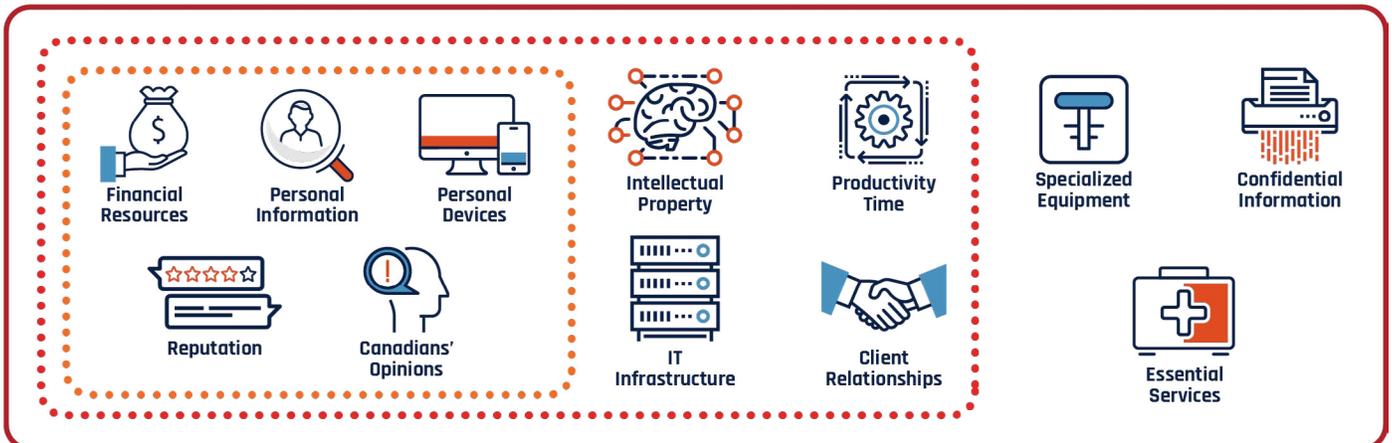
This case demonstrates how an MSP compromise can result in damaging global, cross-sector consequences. In this case, the scope and scale of the compromise helped cyber threat actors obfuscate their motivations and identities, as well as their primary targets of interest.





CYBER THREATS TO CANADIAN CRITICAL INFRASTRUCTURE

TARGETS



Cyber threat activity against critical infrastructure can have consequences far more severe and wide-reaching than activity against individuals and businesses. Cyber incidents affecting Canadian critical infrastructure have the potential to compromise public safety and national security.

We judge that the proliferation of malicious cyber tools has created opportunity for less sophisticated cyber threat actors to attempt to interfere with critical infrastructure. As the number and variety of devices used to support, monitor, and control critical infrastructure become more interconnected, the likelihood of cyber threat actors disrupting critical infrastructure has increased.

For example, cybercriminals have unwittingly compromised critical infrastructure systems while exploiting a vulnerability in a more generic context. We have observed such malware spread uncontrollably, infecting critical infrastructure networks, even when cyber threat actors did not target them specifically.

Critical infrastructure providers are vulnerable to indiscriminate cybercrime activity, but their essential role in daily life means their equipment and services are also potential targets amid hostilities between states. State-sponsored cyber threat actors have conducted cyber espionage against critical infrastructure networks in Canada and allied nations.¹⁹ In Canada, these threat actors have conducted reconnaissance and intelligence-gathering in the energy, aerospace, and defence sectors.

However, at this time, we assess it is very unlikely that state-sponsored cyber threat actors would intentionally seek to disrupt Canadian critical infrastructure and cause major damage in the absence of international hostilities.



WANNACRY

In In May 2017, WannaCry ransomware infected more than 200,000 vulnerable computers in at least 100 countries. Notably, the ransomware spread to 25 facilities in a national health organization that provides emergency services. The incident forced the cancellation of over 19,000 appointments, including surgeries.¹⁷ The Communications Security Establishment and partner agencies have attributed WannaCry to North Korean cyber threat actors.¹⁸

While the cyber threat actors did not target the health service specifically, WannaCry highlights the threat posed by malware to critical infrastructure connected to the Internet and the real world consequences that can follow. It also demonstrates that some cyber activity can have even greater consequences than cyber threat actors may have anticipated. Although the ostensible aim of WannaCry was to collect ransom, its primary effect was to disrupt business operations around the world.

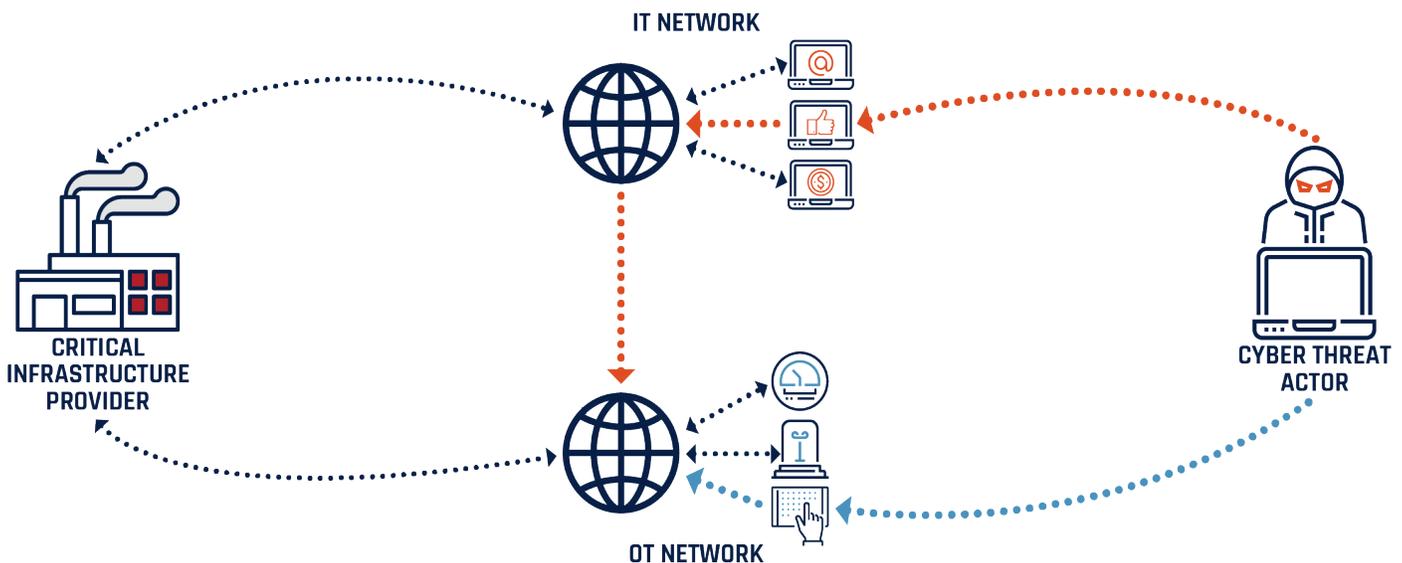


INCREASING CYBER THREAT EXPOSURE

Critical infrastructure providers typically rely on a mix of technologies to manage administrative and industrial processes. They use IT to manage daily business functions and operational technology (OT) to control specialized equipment such as machinery used in complex and dangerous physical environments. Critical infrastructure providers use supervisory control and data acquisition (SCADA) devices to manage their industrial control systems (ICS).

As part of the drive for modernization and efficiency, critical infrastructure providers are continuing to automate their processes and connect IT and OT devices to the Internet. While connecting OT, such as ICS and SCADA devices, to the Internet provides several advantages – for example, remote management – it can also expose critical infrastructure to cyber threat activity. We assess that the proliferation of cyber tools on cybercrime marketplaces has very likely made it easier for cyber threat actors to gain access to critical infrastructure OT.

Figure 9: Cyber threat actors try to access IT and OT of a critical infrastructure provider



CYBER OPERATIONS AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE

In June 2017, the NotPetya malware infected tens of thousands of devices, including those on critical infrastructure networks in Ukraine and around the world. Cyber threat actors introduced NotPetya through a software package for a tax return application widely used by businesses in Ukraine. By including malware into an update for the software, the cyber threat actors infected user devices and the malware spread across networks, encrypting hard drives. NotPetya affected systems in at least 74 countries. Ukraine, in particular, suffered significant disruption to its government, banking, transportation, and telecommunications infrastructure.²⁰ The Communications Security Establishment and partner agencies have attributed NotPetya to cyber threat actors in Russia.²¹

Earlier, in December 2015, cyber threat actors compromised the information systems of energy generation and distribution companies in Ukraine, temporarily disrupting power delivery to 225,000 people. By installing malware on an energy provider's computer system via spear-phishing, the cyber threat actors could remotely cut power. The cyber threat actors then disabled customer service phone lines to prevent customers from reporting the outage. A similar incident occurred in December 2016, when a fifth of the Ukrainian capital Kyiv lost power for an hour.²²

The case demonstrates that critical infrastructure supply chains can become targets during tension or conflict between nation-states. Cyber operations such as those experienced in Ukraine typically require long-term cyber espionage and planning.

Accessing Industrial Control Systems

An industrial control system (ICS) is a type of operational technology that monitors and controls the physical equipment used in critical infrastructure, such as the processes involved in energy generation or the management of a transportation system.

Historically, manufacturers designed ICS devices to have long-service lifetimes, and many legacy systems continue to be used today. Legacy systems were built for safety and functionality, not cyber security. In recent years, secure devices and protocols have emerged and critical infrastructure providers are deploying them on new ICS installations. We assess that cyber threat actors will likely target unsecure devices and legacy systems until aging machinery and software are phased out and replaced.

We assess that a deliberate attempt to compromise an ICS would very likely require in-depth knowledge of proprietary information, such as network design and communications protocols, and an understanding of how the equipment is used in a particular industrial process. To collect proprietary information, cyber threat actors typically need to establish a covert presence and observe network activity over time. However, as inadequately secured ICS are connected to the Internet, they can become vulnerable to less sophisticated cyber threat actors, such as cybercriminals.



ENERGY SECTOR COMPROMISE

In 2017, the Communications Security Establishment alerted partners in the United States to an energy sector ICS cyber compromise. According to officials at the Department of Homeland Security, Russian cyber threat actors reached secure systems and isolated networks, advancing to the point where they could have disrupted power flows in North America. The cyber threat actors exploited relationships between critical infrastructure and trusted third parties that had ICS access for the purposes of updating software and running diagnostic tests. To compromise the third parties, cyber threat actors used relatively simple techniques, such as spear-phishing emails, to learn the login credentials of employees at supplier firms, including much smaller companies.²³

This case demonstrates that critical infrastructure is vulnerable to supply chain compromises. It also shows that a compromise can occur with a low-sophistication technique yet provide a cyber threat actor with access to a powerful ICS. Destructive activity by cyber threat actors can lead to a widespread loss of power, potentially interfering with business operations and essential public services. Since North American energy grids are connected, a major cyber event in the United States or Canada could have disruptive effects in both countries, highlighting the importance of international partnerships.



PUBLIC INSTITUTIONS AND SENSITIVE INFORMATION

We assess that cyber threat activity against public institutions – such as government departments, universities, and hospitals – is likely to persist because of the essential nature of the services and the sensitivity of the information they manage.

Public institutions are also attractive to cyber threat actors because of their close connections with businesses and Canadians. Public institutions hold valuable intellectual property, sometimes belonging to partner organizations such as research centres or private firms.



CANADIAN MUNICIPAL GOVERNMENT RANSOMWARE COMPROMISE

In April 2018, cyber threat actors struck 11 servers belonging to a municipal government in Ontario with a ransomware compromise. The encryption malware used by the cyber threat actors prevented officials from accessing municipal data, disrupting local authorities' ability to operate. The cyber threat actors demanded 11 bitcoin (then \$144,000) to unlock 11 servers. After seven weeks of consultations and negotiations, municipal authorities paid the cyber threat actors three bitcoin (then \$34,950) for four servers holding the most important data. The incident did not compromise any personal information.²⁴

	Ransom Payment	\$34,950
	Computer Consultants	\$37,181
	Physical Security Vendor	\$4,725
	IT Purchases	\$1,901
	Third-Party Software Vendors	\$9,590
	Internal Staff Overtime	\$31,370
	Internal Productivity Losses	\$132,042
	Total Cost of Ransomware Incident	\$251,759

We assess that confidential data will very likely remain an attractive target for cyber threat actors. Canadians provide sensitive information about themselves when they use essential public services with the expectation that their information will be secure. By accessing personal information and threatening its release, cyber threat actors can try to coerce decision makers at public institutions into paying a ransom to protect citizen confidentiality, maintain operations, and defend reputations.

Public institutions also create and collect other kinds of sensitive information of value, which cyber threat actors target for ransom or sale. For example, in order to sell valuable information or conduct espionage, cyber threat actors target details about confidential operations, such as negotiations or deliberations. While foreign intelligence agencies have conducted espionage against federal and sub-national governments for decades, the digitization of government services has created more opportunities to attempt to access confidential information using cyber capabilities.

Nation-state adversaries have the greatest capability and intent to conduct cyber threat activity against Canadian public institutions. State-sponsored cyber threat actors vary in sophistication and it is likely that some advanced actors can operate undetected. Cyber threat activity against Canadian public institutions occurs most often when Canada is a global research leader, or involved in sensitive international or bilateral issues.

We assess that nation-states around the world are continuing to invest in their cyber capabilities with the intent of advancing their national security and economic objectives.

CONCLUSION

The cyber threat environment in Canada is always changing. We expect cyber threat actors to shift their methods and targets based on their evolving priorities, motivations, and capabilities.

In this assessment, we identified current trends in the cyber threat environment. Wherever possible, we highlighted the likelihood of cyber threat activity and examined how it can affect Canadians, as well as Canadian businesses and critical infrastructure.

In general, most of the cyber threats that we discussed can be mitigated through awareness and best practices in cyber security and business continuity. Cyber threats and influence operations 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.

As the National Cyber Security Strategy recognizes, Canadian citizens, businesses, and critical infrastructure operators need to have confidence in the cyber systems we rely on every day. We are making a difference. The Cyber Centre approach of security through collaboration brings together expertise from government, industry, and academia to tackle the toughest cyber challenges that Canada faces. Working together, we can make Canada more resilient against cyber threats.

USEFUL RESOURCES

For more information about mitigating cyber threats, we strongly encourage visiting:

- [An Introduction to the Cyber Threat Environment](#)
- [Top 10 IT Security Actions](#)
- [Cyber Centre's advice on Cyber Hygiene](#)
- [Cyber Centre's advice on Mobile Security](#)
- [Get Cyber Safe Campaign](#)
- [Little Black Book of Scams](#)
- [Security Review Program Fact Sheet](#)
- [Cyber Security Considerations for Contracting With Managed Service Providers](#)
- [Technology Supply Chain Guidelines \(TSCG-01\)](#)
- [Malicious Cyber Activity Targeting Managed Service Providers](#)
- [Protect Yourself Online](#)
- [Learn More about Assembly Line](#)
- [Whitelist applications](#)
- [Protect your devices and networks](#)
- [Implement architectural controls for network segregation](#)
- [Keyloggers and Spyware \(ITSB-49\)](#)
- [How to spot misleading information online and what to do about it](#)
- [Joint Report On Publicly Available Hacking Tools](#)
- [Spotting malicious e-mails](#)
- [Phishing](#)
- [Canada.ca/taxes-fraud-prevention](#)
- [Doppelganger Campaigns and Wire Transfer Fraud](#)

ENDNOTES

- ¹ Critical infrastructure refers to the processes, systems, facilities, technologies, networks, and services essential to the health, safety, security, and economic well-being of Canadians and to the effective functioning of government. [Public Safety Canada](#). 12 June 2018. Accessed September 2018.
- ² In this assessment, we use the term cybercrime to refer to criminal activity involving a network or network-connected device.
- ³ [United States Department of Justice](#). 13 December 2017. Accessed September 2018; and Perloth, Nicole. [The New York Times](#). 21 October 2016. Accessed September 2018
- ⁴ [Cyber Threat Alliance](#). 19 September 2018. Accessed September 2018.
- ⁵ [Canada Revenue Agency](#). 31 August 2018. Accessed September 2018.
- ⁶ Extortion refers to unlawfully obtaining money, property or services from a person or institution through threats or force.
- ⁷ [Canadian Anti-Fraud Centre](#). August 2018. Accessed September 2018.
- ⁸ [Canadian Centre for Cyber Security](#). June 2017.
- ⁹ Rocha, Roberto. [CBC News](#). 3 August 2018. Accessed September 2018. Original dataset available at: [Data Source](#).
- ¹⁰ [Canadian Internet Registration Authority](#). 22 March 2018. Accessed September 2018.
- ¹¹ [Royal Canadian Mounted Police](#). 15 January 2018. Accessed September 2018.
- ¹² [The Globe and Mail](#). 18 June 2018. Accessed September 2018; Evans, Pete. [CBC News](#). 28 May 2018. Accessed September 2018; and [Canadian Financial Group](#). 28 May 2018. Accessed September 2018.
- ¹³ A smart phone or laptop computer may have been designed in one country, the raw materials and specific components like the screen, microphone, and camera can come from companies around the world, and the device itself could have been assembled in yet another location before reaching a consumer in Canada.
- ¹⁴ 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 [National Institute for Standards and Technology](#). April 2015. Accessed September 2018.
- ¹⁵ Corera, Gordon. [BBC News](#). 26 July 2018. Accessed August 2018; and Menn, Joseph. [Reuters](#). 18 September 2017. Accessed September 2018.

- ¹⁶ [PricewaterhouseCoopers United Kingdom](#). April 2017. Accessed September 2018; and Nish, Adrian and Tom Rowles. [BAE Systems](#). 3 April 2017. Accessed September 2018.
- ¹⁷ [National Audit Office \(United Kingdom\)](#). 25 April 2018. Accessed September 2018.
- ¹⁸ [Communications Security Establishment](#). 19 December 2017.
- ¹⁹ [United States Computer Emergency Readiness Team \(US-CERT, Department of Homeland Security\)](#). 15 March 2018. Accessed September 2018.
- ²⁰ Perloth, Nicole, et al. [The New York Times](#). 27 June 2018. Accessed September 2018.
- ²¹ [Communications Security Establishment](#). 15 February 2018.
- ²² [BBC News](#). 26 February 2016. Accessed September 2018; and [BBC News](#). 11 January 2017. Accessed September 2018.
- ²³ Smith, Rebecca. [The Wall Street Journal](#). 24 July 2018. Accessed September 2018; and [United States Computer Emergency Readiness Team \(US-CERT, Department of Homeland Security\)](#). 15 March 2018. Accessed September 2018.
- ²⁴ [CTV News](#). 24 July 2018. Accessed September 2018; and [Canadian Municipal Government Meeting Agenda](#). 24 July 2018. Accessed September 2018.