Torkin Manes
Barristers & Solicitors

Article

Technology, Privacy & Data Management

December 2020

Think before you click! New cyberthreat assessment published

Canadian Centre for Cybersecurity provides new analysis and forecasts on threats to Canadians

By Lisa R. Lifshitz

In November 2020 the Canadian Centre for Cybersecurity ("Cyber Centre") issued its second National Cyberthreat Assessment document (the "Report"), which assesses the most pressing threats to cybersecurity in Canada today. The document updates the National Cyberthreat Assessment 2018 (NCTA 2018), analysing the interim years and providing forecasts until 2022, and its analysis of trends and predictions makes for interesting if rather grim reading.

The Report noted that as technologies such as artificial intelligence (AI), the internet of Things (IoT), the Industrial Internet of Things (IIoT), and cloud computing play an increasingly critical role in personal, commercial and industrial activities in Canada, such growing reliance on online activities has increased the susceptibility to threat activity. Cybercriminals motivated by financial gain remain the number 1 threat to most Canadians – think ransomware attacks, theft of personal, financial and confidential information, and distributed denial of service [DDoS] attacks – followed by state-sponsored actors motivated by economic, ideological and geopolitical goals.

These state-sponsored individuals and groups often possess even more sophisticated tools and use them to conduct cyberespionage, intellectual property theft, online influence operations and disruptive cyberattacks. While "hacktivists" and other thrill seekers still pose some threat, the Report judges them as a less common, less potent menace to average Canadians.

Identified trends in cybersecurity

The Report identified five trends that will drive the evolution of the cyberthreat landscape in Canada:

1. Physical safety of Canadians is more at risk. The most pressing threats result from the convergence of operational technology (OT) with information technology systems (IT). Canada's critical infrastructure — e.g., energy, power, or medical devices — is increasingly controlled by embedded computers that are more susceptible to cyberthreat activity when connected to the internet. Operational technology — used to control physical processes such as pipeline operations, boiler activities and dam openings — was not designed to be connected to the internet, though now it is for a variety of reasons.

   Yet not all these systems have adequate cyber protections, and the OT/IT convergence increases the risk of cyberthreat activity reaching OT systems. A 2019 survey found that 68 per cent of manufacturers plan to increase their investment in IT-OT convergence solutions for their organizations over the next two years. The Report also mentions the heightened risk to Canadians from the targeting of smart cities and of IoT devices such as personal medical devices and internet-connected vehicles.

2. More economic value is being put at risk. Soaring cybercriminal activity, including by state-sponsored cybercriminals, is hurting Canadian individuals and businesses. This trend is expected to grow, including more ransomware attacks and increased efforts by certain states to steal intellectual property and proprietary business information. This has been spurred by the COVID-19 pandemic, which hastily forced individuals and businesses to work remotely without due regard to cyber-protection. Think of stressed employees accessing sensitive company intellectual property/data using their personal devices and home Wi-Fi networks that may be poorly secured in comparison to corporate IT infrastructure, making thefts easier. The Report noted that commercial cyberespionage against Canadian companies is ongoing across a range of fields, the Report noted, including biopharmaceuticals, aviation, technology and AI, and energy.

3. More collected data increases privacy risk. Canadians love their smartphones, smartwatches, computers, banking apps, medical devices, fitness trackers and home alarms, all of which generate huge amounts of location and other personal and personal health information. Since much of this data is shared online, it becomes highly vulnerable to cyberthreat actors via increasing numbers of data breaches or misuse by the companies or foreign governments that collect it. The Office of the Privacy Commissioner of Canada recorded 680 data breaches affecting 28 million Canadians in the year ending November 1, 2019. In 2019, breaches at financial institutions Desjardins Group and Capital One led to the exposure of such personal information as names and birthdates, social insurance numbers, contact information, banking details, credit scores, transaction data, and bank account numbers. Additionally, advances in technology make it difficult to maintain online data anonymity and prevent previously anonymous data to be linked to other datasets and de-anonymized, since Big Data matches bits and pieces about users and compiles profiles of them and their behaviours that can make them identifiable.

4. Advanced cyber tools and skills are accessible to more threat actors. Cyber criminals are getting smarter, more talented and have better tools than ever before. Commercial markets for cyber tools, and a global talent base of hackers for hire, have meant less time is needed for states to build cyber programs. The number of those with cyber programs has increased (the Council on Foreign Relations' current list of countries suspected of sponsoring cyber operations stands at 33).

   It's now easy to find online marketplaces on the dark web that allow vendors to sell specialized cyber tools and services that users can purchase and use to commit cybercrimes such as website defacement, espionage, DDoS attacks, and ransomware attacks. The global market for cyber products and services is projected to grow from approximately $204 billion in 2018 to $334 billion in 2023. Cryptocurrency, as a means of exchanging and laundering money with greater anonymity, has also facilitated the activities of cybercriminals and states.

5. The internet is at a crossroads. The Report observes that certain countries see internet governance as a matter of state sovereignty, with a high focus on domestic stability and national security. These countries prefer an internet that will allow them to track and surveil their citizens, censor information at will, feed their citizens misinformation and arrest dissidents, rather than use the freer, multi-stakeholder approach preferred by Canada that seeks wide participation from various governments, industry, civil society and academia. This can and will have an impact on how the internet will be governed.

Threats to Canadians

The Report also cites the increasing trend of online foreign influence and the attempts to disrupt domestic events such as elections and sway public opinion on national and international events. States have developed cyber tools to carry out large-scale online influence activities, whether through social media efforts, legitimate advertising or information-sharing tools. Most disturbing is the use of “deepfake” technology that creates realistic-looking fake videos of events and public figures, which sows additional layers of uncertainty and confusion for the targets of disinformation campaigns. Deepfake technology can swap faces, produce a video of a full person from scratch, and clone existing human voices.

The Report canvassed the most virulent threats to Canadian individuals and corporations. Individually, Canadians remain highly susceptible to fraud and extortion by cyberthreat actors, losing over $43 million to cybercrime fraud in 2019, according to statistics collected by the Canadian Anti-Fraud Centre; actual figures may be much higher. Individuals are tricked into clicking on malicious links or attachments from seemingly legitimate organizations such as government agencies, banks or even law firms, and which then download malware onto their devices.

Cyber scammers have created fake websites and online ads that offer cheap immigration services, guarantee high-paying jobs for new immigrants, or require fees to access “important forms” from seemingly official government sites. The Report notes that 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. Extortion methods include threatening victims with cyberattacks, stealing incriminating information from victims and then blackmailing them, creating fake profiles on social media and dating websites that lure victims into online relationships that facilitate extortion and fraud.

Corporate attacks

At the corporate level, cyber criminals have been busy targeting both online and in-person payment systems, exploiting supply chain vulnerabilities. Canadian organizations of all sizes, private- and public-sector, are increasingly vulnerable to fraud, ransomware attacks and the theft of proprietary information or customer and client data.

In recent years cybercriminals have shrewdly focussed on “big-game hunting,” targeting large organizations that will not (or cannot) tolerate sustained, major disruptions to their networks and are therefore willing to pay large ransoms to restore their operations and data. This has driven up the number and value of ransom demands, with the average demand increasing by 33 per cent since Q4 2019 to approximately $148,700 in Q1 2020, with “increasingly common” ransom demands over a million dollars. For example, the Report noted that in October 2019 a Canadian insurance company paid $1.3 million to recover 20 servers and 1,000 workstations following a ransomware attack.

In 2019 and 2020 cybercriminals also recognized the value of many Canadian health organizations. Three Ontario hospitals were the victims of ransomware attacks in October 2019, a Canadian diagnostic and specialty testing company was compromised in December 2019, and in early 2020 a medical company in Saskatchewan was hit. Health sector organizations are popular ransomware targets for cybercriminals given their financial resources and the fact that they are more likely to pay ransoms than risk network downtime that can have life-threatening consequences for patients.

Since 2018 cyberthreat actors have increasingly deployed social engineering techniques to target organizations including the so-called business email compromise (BEC). This involves sending email messages (allegedly from high-level executives or trusted third parties) designed to trick employees in the target organization into directly transferring funds to cyberthreat actors. The technique has exploited COVID-19 uncertainties to successfully target victims not only in business but in religious, educational and not-for-profit organizations. Because of the simplicity and profitability of social engineering techniques their use will no doubt continue; 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, the Report stated.

Lastly, the Report highlighted the growing exploitation by cybercriminals of various retail payment systems, including “formjacking,” or stealing credit card details and other information that victims enter on e-commerce sites. Approximately 4,800 websites were victims of formjacking each month in 2018, including those of airlines and ticket sellers. In 2019, formjacking attacks occurred at more than 200 campus stores at universities and colleges in Canada and the U.S., and the Report forecasts this trend will

likely increase over the next two years as Canadians increasingly rely on e-commerce due to the COVID-19 pandemic.

How best to combat the above? The Report contains a number of links to some very useful “best practices” and resources of the Cyber Centre, which is further available to parties wanting a deeper dive.

Perhaps equally helpful, however, is the Cyber Centre’s view that many cyberthreats can be mitigated through a combination of awareness and best practices in cybersecurity and business continuity. In short, Canadians need to not only correct their technological vulnerabilities, but to address those behaviors that give rise to exploitation by cybercriminals, whether through additional cyber training or other means to increase cyber resilience.

As I have written before, as a first step, think before clicking and we will all be better off.

Author

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Lisa R. Lifshitz is a partner in Torkin Manes’ Business Law Group, specializing in technology and privacy law, and is the leader of the firm’s Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the immediate past president of the Canadian IT Law Association.