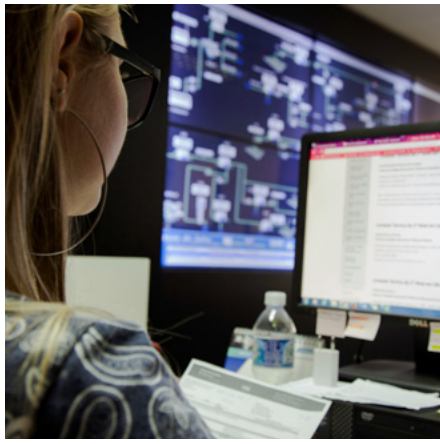
Grant Thornton

2021-2022

Cybersecurity in Canada

Evolving threats and practical defences




Lead IT Technician

Contents

The past two years have continued to redraw the Canadian cybersecurity landscape, from the massive infrastructure vulnerabilities exemplified in the SolarWinds attack to ongoing pandemic-related volatility.

We've seen significant advances in technology, including the continued move toward the digital workplace; the mass shift to online learning; the rise of contactless services and the gig economy; and cutting-edge developments in health care and the life sciences, including the development of vaccines in record time and the adoption of virtual health care. While these developments are to be celebrated, they should also be treated with renewed vigilance around those who seek out vulnerabilities in the technologies and mindsets that are shaping the new normal.

Retrospective (2021)

This report will offer a two-fold examination of the Canadian cybersecurity landscape to contextualize and explain immediate and imminent threats to your organization's cybersecurity and the evolving nature of the threat actor. We first offer a retrospective examination of the key cybersecurity issues we noted in 2021, including:

- Responding to the pandemic
- Threats to operational technology
- The redoubling of ransomware
- Underfunded and understaffed: the cybersecurity staffing problem

Predictions (2022)

We then offer some predictions and guidance on what Canadian businesses should expect and how to help protect their assets in 2022 and beyond, including:

- Operational technology will continue to be a target
- Fix your cybersecurity staffing problem
- Ransomware: an ongoing epidemic
- Supply chains will continue to be targeted
- Eliminate a static approach to cybersecurity
- Implications of the shift to the cloud

2021: A year defined by expanding threats and vulnerabilities

2021 saw significant cybersecurity-related events, from large-scale breaches to the use of ransomware by criminal groups and nation states. This includes the attack on the province of Newfoundland and Labrador's health system, which is considered the largest breach in Canadian history; phishing attacks using the pandemic as a lure; and opportunistic attacks against organizations trying to save their businesses by transitioning to e-commerce.

This protracted period of change and upheaval—compounded by a critical shortage of qualified cybersecurity resources—provided the perfect conditions for increasingly agile and brazen threat attackers to conduct operations.

Responding to the pandemic

As pandemic-related restrictions extended over the past year, organizations identified that their budgets and governance models could not address the current cybersecurity landscape. Senior leadership and boards admirably focused on trying to keep their workforce healthy and their businesses from collapsing, and this meant that while cyber security risks were better understood and prioritized, there was no time or resources to invest. In many cases, executives made major strategic decisions—including moving to the cloud and transitioning critical IT functions to third parties—without consulting with their cybersecurity team. Many organizations lacked a documented pandemic response plan and relied on business continuity processes that could not address the effects of a global pandemic, including swaths of IT resources—the most critical players in assessing risk—being unable to work due to illness and workforces having to move to remote settings.

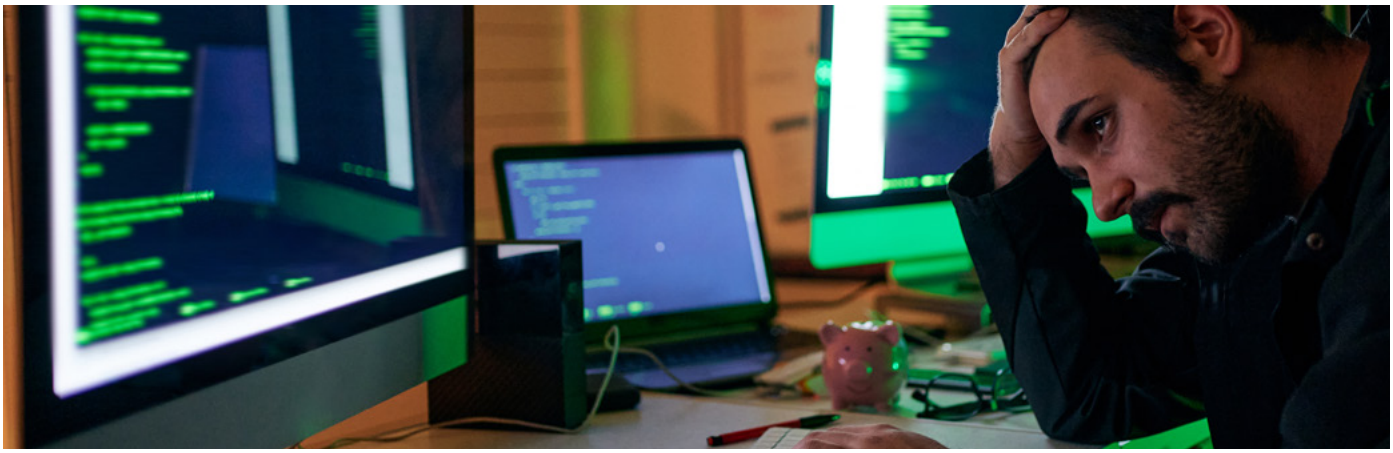
We also noted organizations undergoing large transformational projects in response to the pandemic, including moving traditional brick-and-mortar operations to e-commerce and transitioning critical business applications such as an ERP, e-mail, document sharing and collaboration to the cloud. In many cases, these projects did not seek the typical cybersecurity risk assessments or were not appropriately funded to ensure that cybersecurity controls were in place at the time of deployment. Given the scope and scale of threats, it should come as no surprise that a recent survey of 3,040 Canadian Federation of Independent Business (CFIB) members across Canada[1] found that nearly a quarter have experienced cyber-attacks since mid-2020, the time when many businesses had to increase their online presence— or start it from scratch.[2]

3,040 Canadian Federation of Independent Business (CFIB) members across Canada found that nearly a quarter have experienced cyber-attacks since mid-2020.

Threats to operational technology (OT)

Attacks on operational technology (OT) made headlines throughout 2021, from the attack on the Colonial Pipeline that caused a complete shutdown of their infrastructure to the breach of the Oldsmar water plant in Florida due to weak remote access controls. Operational technology—also known as industrial control systems (ICS)—is the hardware and software that monitors and controls industrial processes in a range of sectors, including chemical plants, power utilities, health care and manufacturing. Although many of these known cyberattacks occur in the United States, Canada is not immune. The Communications Security Establishment (CSE) said it's aware of 235 ransomware incidents against Canadian victims[3] from January 1, 2021 to November 16, 2021. More than half of those targets were critical infrastructure providers, including those in the energy, health care and manufacturing sectors.

We noted that targeted attacks appeared to have outweighed opportunistic attacks, with cyber-attackers adding ransomware and extortion to their arsenal. We also continued to see attacks that originated on IT networks using well-known vectors, such as phishing and the exploitation of known vulnerabilities in systems. Given the weak network segmentation between IT and OT networks, attackers are easily able to infiltrate the OT environment. As we saw with the Oldsmar attack, engineering workstations with connectivity into both the IT and OT environments proved to be a popular method for attackers to breach an ICS environment. We also saw many key players in the industrial equipment space—including Schneider Electric, Rockwell, and Siemens—releasing numerous advisories for identified vulnerabilities. Updating OT equipment isn't an easy and quick process for many critical infrastructure organizations—and public advisories leave known vulnerabilities open to attack.



The redoubling of ransomware

Ransomware continued to be a popular attack vector for criminals due to the simplicity in sourcing malware, an abundance of exposures for attackers to initially breach the victim's system and the high likelihood of a payout.

Our work on ransomware-related attacks during the past year has shown a shift in the methods used by many criminal organizations when seeking a ransom. The target of choice continued to move away from consumers and/or smaller organizations to medium- and large-sized enterprises, which is largely attributable to the increased opportunity that the victim will have the means to ensure payment of the ransomware. Criminals are also ruthlessly targeting more vulnerable organizations such as hospitals, critical infrastructure, and other organizations where an attack could have a harmful effect on the business—and human life. For example, the backdrop of a devastating pandemic hasn't stopped attackers from seeking ransoms from hospitals while they struggle to meet the demands of patients. While the overall number of attacks has dropped, we have noted that the potential for damage from these targeted attacks is much higher, as seen in the devastating ransomware attack on the Humber River Hospital[4].

More organizations have invested in cyber-insurance to handle the fallout from an attack by paying the ransom as opposed to attempting to fully restore or even seek bankruptcy. Although this continues to be the method of choice, we have seen that given the cost of ransoms and the indirect costs of negotiation, forensics and recovery, insurance companies are imposing requirements such as the use of two-factor authentication, investing in endpoint detection and response (EDR) tools, and secure remote access. Insurance companies are deciding to underwrite organizations based on whether intelligence exists that the company may have previously been subject to a breach or even targeted by cyber-attackers. Although these are good cyber-hygiene tactics, many organizations are not prepared to implement these solutions on a whim and this may affect their likelihood of obtaining insurance going forward.

From a technique perspective, we have noted that cyber-attackers have continued to take advantage of ransomware-as-a-service, with criminal groups such as Conti, REvil, and others franchising their malware capabilities to attackers, thus eliminating the need to develop malware on their own. The concept of double extortion has also grown. Given increased preparedness by organizations to weather the ransomware storm—including secure cloud-based backups of their data—attackers have had to shift their tactics. For example, we now see attackers threatening to encrypt victim systems after also stealing a copy of sensitive information—including customer PII and intellectual property—and then threatening to share this on the dark web with the criminal underground. This is often more detrimental to the victim than the ransomware itself.

"Like many other IT executives, ransomware is a type of breach that keeps us up at night. As much as we can prepare for something like that, I still believe it could have a devastating effect on our company. Too many large organizations I thought would never be at risk have been hit. It is extremely scary."

-Senior Director, network operations, national financial services company

Underfunded and understaffed: the cybersecurity staffing problem

The cybersecurity budget in many organizations is low relative to overall IT spend despite the growing threat of cyber-attack, while current shortages of experienced cybersecurity professionals remain high. Cybersecurity has not been immune to a global skills shortage and people embracing the new normal with a change of employment, including moves from consulting to industry or vice-versa, changing careers, or taking early retirement. Many are leaving the profession to return to their roots as developers or network engineers, in many cases to avoid the stress that comes with the growing potential for a breach, insufficient budgets, and staffing shortages.

(ISC)[2]--the world's largest non-profit association of certified cybersecurity professionals—complied figures by conducting interviews with 3,200 security professionals worldwide for its most recent Cybersecurity Workforce Study[5] report. The report indicated that the global cybersecurity workforce currently stands around 2.8 million, and that the global demand of a little over 4 million is beyond our current capacity. The numbers are startling and indicate an ongoing staffing crunch: we need to add an additional 145% trained cybersecurity professionals to meet our needs, and unfilled positions grew by 2.93 million from the previous year of reporting.

The cybersecurity staffing problem has also led to an increase in the overall cost in securing an experienced cybersecurity resource, both with the expense of hiring an individual and the time and cost of ensuring their training is in line with new threats. According to the Dice 2021 Tech Salary Report[6]—which breaks down top IT salaries based on location, experience, and skill sets—cybersecurity was one of the highest paying IT jobs in 2021 based on salary growth. The Cyber Security Engineer role ranked in the top fastest-growing IT salaries in 2021, with a salary that increased to an average of $134,340 USD (an increase of 4.3 per cent).

We need to add an additional

145%

trained cybersecurity professionals to meet our needs

Looking ahead to 2022: An increasingly agile and complex threat actor

2021 saw continued targeting of businesses via their major supply chain vendors—exemplified in the Kaseya and SolarWinds breaches—and we expect to see more of the same in 2022. Canadians also suffered the wrath of complex, foreign nation-state-based campaigns such as that perpetrated by Hafnium targeting zero-day vulnerabilities in Exchange, the popular Microsoft mail server. According to the Canadian Centre for Cyber Security (CCCS)[7], "These vulnerabilities are being leveraged to gain a foothold within an organization's network for malicious activity which includes but is not limited to ransomware and the exfiltration of data."

2022 will bring continued stress for organizations trying to protect their assets and those of us who are trying to protect them from increasingly sophisticated campaigns. Threat actors are progressively brazen and agile—and Canadian businesses of all sizes will not be immune to new strategies to derail much of the cybersecurity protection that they have diligently put in place.

Operational technology will continue to be a target

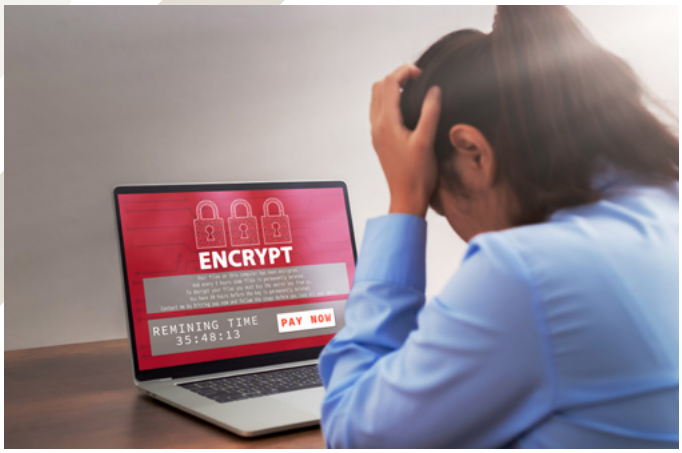
Cyber-attackers are all too aware that the security of most OT environments is generally weak—exemplified in 2021 with Colonial Pipeline, Oldsmar Water and JBS Meats—and we expect this awareness to grow in 2022. We will also see more ransomware-related attacks of opportunity against vulnerable OT systems and weak remote access controls. The public relies on OT systems to ensure we have clean drinking water, energy for our homes and a safe food supply. Disruptions to critical OT systems mean that organizations cannot ensure that the public can safely rely on their products and services. While many cybersecurity-related projects were put on hold due to cost, organizational restructuring and workplace change, organizations operating OT systems must continue their pre-pandemic convergence of IT and OT environments to ensure that consistency from a cybersecurity perspective. Key areas of focus for organizations in 2022 include key controls related to privileged access management, remote access (both from the enterprise network and outside the enterprise), and network monitoring and vulnerability management.

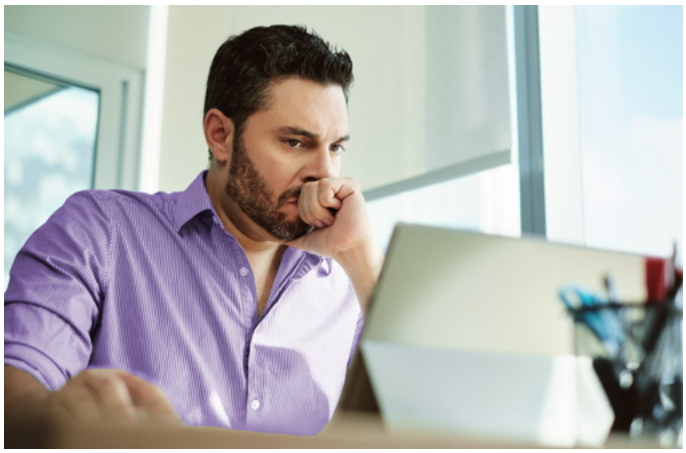
Fix your cybersecurity staffing problems

Organizations should be aware that the concurrent demand for and shortage of experienced cybersecurity resources has resulted in dramatic salary increases—and Canada is not immune. While this can exceed many organizations' budgets, they must adapt. Moving forward, having a sufficient CAPEX budget alone to purchase technology will not be enough to sustain an organization's cybersecurity needs. We suggest a four-pronged approach: provide cybersecurity training to some of your experienced IT staff; pivot to meet the salary needs of experienced cybersecurity professionals; find innovative ways to keep attrition levels low; and fill gaps with outside assistance from consultants and managed security service providers.

"More and more cybersecurity requirements are becoming mandatory among hospitals as we become more integrated."

– VP Operations, regional hospital





Ransomware: an ongoing epidemic

Ransomware is not going away in 2022. If anything, expect to see more of it given its pervasiveness in 2021. New criminal ransomware gangs will emerge, new ransomware-as-a-service options will be available and new variants will infect our systems. Although the infiltration techniques we saw in 2021—including phishing, insecure remote access and targeting vulnerable systems—will not change, attackers will become more and more brazen, targeting major critical infrastructure, governments, health care and businesses. Expect double-extortion methods to continue where organizations will look to protect their data from distribution over the dark web.

Organizations must adopt strong controls to counter these ongoing threats, including:

1. Frequent patching of vulnerabilities
2. Ensure remote access is limited to VPN and requires two-factor authentication
3. Testing of the organization's response processes through simulation and table-top exercises, including what to do first and who to call in the event of a systems shutdown
4. Adoption of the principle of least privilege: limit user access to what they need to perform their job and ensure endpoints have strong, regularly updated protection

Supply chains will continue to be targeted

Just as we saw with the SolarWinds and Kaseya breaches, Canadians should expect their supply chains to be ongoing targets, whether attacks against the code-base of commonly used applications or breaches of suppliers with access to networks such as managed service providers. Organizations must perform their due diligence to ensure that their suppliers adhere to the same strict cybersecurity standards. Trust is not enough to eliminate the requirement for least privileged access to systems, the use of multi-factor authentication and protection of privileged credentials. Organizations should look to ensure that vendors follow strict cybersecurity processes and that they can audit them at any time. Look to implement privileged access management (PAM) systems to control access to key systems and ensure that vendor-related breaches are part of the organization's incident response plan.

"I don't think anyone is ever prepared for a cyber-breach until they have gone through it personally. We have a cyber security framework in place and are doing a lot of good things, but depending on the origin of the breach, the lack of a true SIEM would be problematic."

– Director, IT Service, large crown corporation

Eliminate a static approach to cybersecurity

The threat landscape will continue to grow in 2022, and organizations must continue to be agile and proactive to defend their assets from cyber-attacks. Simply hiding behind a firewall is not enough. Going forward, we suggest that organizations move away from seeing cybersecurity as a discrete concern by implementing a range of methods to protect their assets—and, by extension—their money, data, reputation, and operations. This should include continual training and table-top exercises; threat hunting, or proactively searching networks and systems for suspicious activities; focusing on behavior or tactics, techniques and procedures (TTPs) and not simply indicators of compromise such as known malicious IP addresses and URLs; and continually collecting security-related telemetry from key systems for analysis.

Implications of the shift to the cloud

The rise of organizations migrating to the cloud in 2021 will continue in 2022. In 2020, the IDC surveyed 100 Canadian companies[8] and noted that 90 per cent had adopted at least one SaaS product, with 35 per cent moving applications to the cloud for better security and reliability. Although cloud offerings can be of great value to organizations wishing to untether themselves from physical, on-premise systems, organizations moving e-mail and collaboration or key workloads to the cloud must ensure that they are aware of the shared responsibility that the cloud brings. Most cloud providers will make available numerous security-related capabilities, but in many cases, it's up to the organization to implement them. Organizations need to ensure that their security posture adapts to meet new cloud-related cybersecurity threats.

90%

of 100 Canadian companies that were surveyed in 2020 had adopted at least one SaaS product, with

35%

moving applications to the cloud for better security and reliability.

Have questions? Let us help.

Wherever your organization is on its cybersecurity journey—from initial planning to robust solutions around data protection, strategy discussions, and systems testing—we're here to help.

Peter Morin

Principal, National Cybersecurity leader

About the author

With over 25 years of experience, Peter's unique expertise ranges from industrial and control system (ICS) security, network security architecture, threat hunting and red-teaming to cloud security, incident response and computer forensics.

Peter has held senior positions with numerous organizations, including a global cybersecurity consulting firm, a national telecommunications and media company, a Fortune 500 cloud-computing company, a recognized cybersecurity software company and a major US defense contractor.

Peter is originally from Montreal, and now lives with his family in Halifax, Nova Scotia.

Peter Morin
Peter.Morin@ca.gt.com
+1 902 421 1734

Endnotes

1 https://content.cfib-fcei.ca/sites/default/files/2021-02/Cyber-Fraud-in-Small-Business.pdf
2 https://www.cfib-fcei.ca/en/media/news-releases/cyberfraud-growing-concern-small-businesses-pandemic-forces-them-digitize
3 https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021
4 https://globalnews.ca/news/7963652/humber-river-hospital-ransomware-attack-toronto/
5 https://www.isc2.org/Research/Workforce-Study
6 https://insights.dice.com/technology-salary-reports/
7 https://cyber.gc.ca/en/alerts/active-exploitation-microsoft-exchange-vulnerabilities
8 https://www.idc.com/ca/blog/detail?id=e87562689df34b9d3598

Grant Thornton

grantthornton.ca

Audit | Tax | Advisory

About Grant Thornton LLP in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. We help dynamic organizations unlock their potential for growth by providing meaningful, actionable advice through a broad range of services. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member and correspondent firms operate in over 100 countries worldwide.