Secure Smart Cities

Making Municipal Critical Infrastructure Cyber Resilient

April 2022

Stephanie Tran | Sharan Khela | André Côté

cybersecure policy exchange

Powered by RBC

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

Ryerson Leadership Lab

The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.

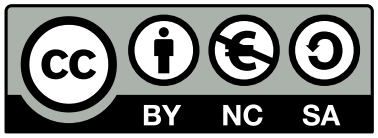
Supported in part by:

Canada Infrastructure Bank

The Canada Infrastructure Bank (CIB) is a federal crown corporation working in partnership with governments, Indigenous communities and the private sector to invest $35 billion in infrastructure that benefits Canadians. By attracting and leveraging private sector and institutional investment in revenue-generating infrastructure projects in the public interest, the CIB is building a portfolio of investments in key sectors including transit, clean power, green infrastructure, trade & transportation and broadband that will foster economic growth, connect Canadians and contribute to the sustainability of infrastructure in Canada. As part of its investment approach, the CIB supports the development of innovative research that can lead to better informed policy and investment choices.

How to Cite this Report
Tran, S., Khela, S., & Côté, A. (2022, April). *Secure Smart Cities: Making Municipal Critical Infrastructure Cyber Resilient*. Cybersecure Policy Exchange. https://www.cybersecurepolicy.ca/secure-smart-cities.

350 Victoria St, Toronto, ON M5B 2K3



Design
Zaynab Choudhry

Copy-editing
Cathy McKim

Contributors
Nour Abdelaal, Policy Analyst, Cybersecure Policy Exchange
Sam Andrey, Acting Executive Director, Ryerson Leadership Lab
Karim Bardeesy, Executive Director, Ryerson Leadership Lab
Sumit Bhatia, Director of Innovation and Policy, Rogers Cybersecure Catalyst
Zaynab Choudhry, Design Lead
André Côté, Acting Director of Policy & Research, Ryerson Leadership Lab
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Sharan Khela, Policy Assistant, Ryerson Leadership Lab
Mohammed (Joe) Masoodi, Senior Policy Analyst, Cybersecure Policy Exchange
Ana Qarri, Policy Analyst, Cybersecure Policy Exchange
Yuan Stevens, Policy Lead, Cybersecure Policy Exchange
Stephanie Tran, Policy Analyst, Cybersecure Policy Exchange

Our work is guided by these core principles:

- Responsible technology governance is a key to Canadians' cybersecurity and digital privacy.
- Complex technology challenges call for original insights and innovative policy solutions.
- Canadians' opinions matter, and must inform every discussion of technology policy.
- Cybersecurity needs to be explained and made relevant to Canadians, and cannot be relegated
- to language and concepts accessible only to experts.
- Canadian institutions matter, and must evolve to meet new cybersecurity and digital privacy
- risks to maintain the public trust.
- Harms, inequities and injustices arising from the unequal use or application of technology must be confronted, wherever they exist or could arise.

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange
For more information, visit: https://www.cybersecurepolicy.ca/

Executive Summary

Critical infrastructure, like energy, water and transportation systems, are increasingly being connected to the internet to increase automation, facilitate remote monitoring and drive efficiency. Despite its benefits, internet connectivity has also made critical infrastructure systems more vulnerable to cyber threats. This report examines the unique challenges and needs of Canada's municipalities for securing their critical infrastructure from cyber threats, developed through a literature and jurisdictional review, along with interviews and a round table with experts.

Key challenges faced by municipalities regarding the cybersecurity of their critical infrastructure include:

- **Increasing cyber attacks targeting municipalities and critical infrastructure:** In 2021, the majority of ransomware victims in Canada were critical infrastructure providers. The scale, frequency and sophistication of ransomware and supply chain attacks continue to cause major disruptions to critical operations.
- **Constrained funding and aging assets:** Underinvestment in critical infrastructure has left municipal budgets stretched to protect these assets from physical threats, nonetheless digital ones. This lack of funding has delayed the replacement of legacy systems, which are more susceptible to cyber attacks.
- **Shortage of cybersecurity talent:** The industry is struggling to hire and retain security labour, and the competitive market puts smaller municipalities at a further disadvantage.
- **Lack of cybersecurity in traditional emergency management:** Emergencies resulting from cyber-physical incidents do not fit into traditional emergency management structures, leaving a lack of clarity on how such emergencies should be prepared for and responded to.

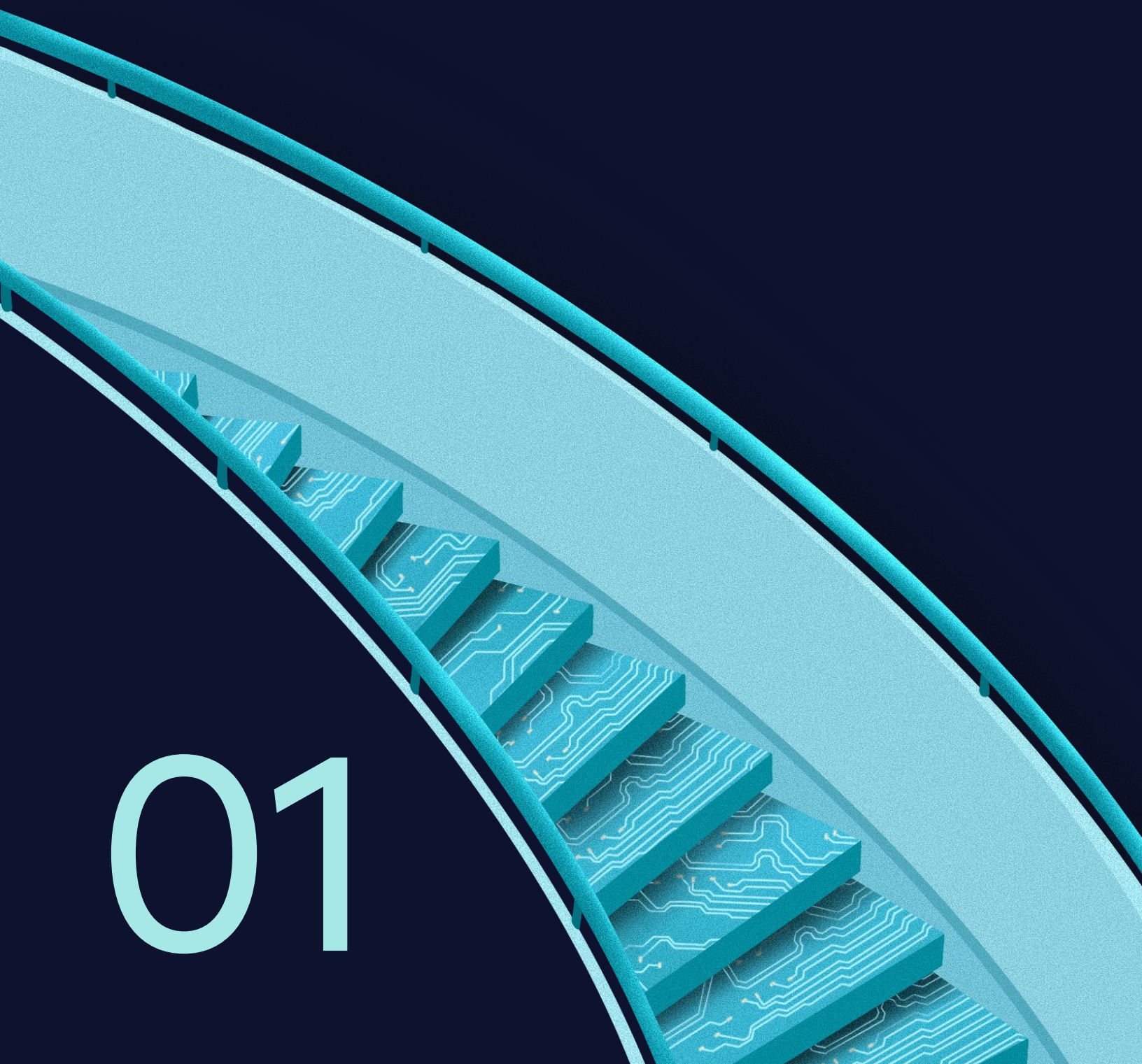
Promising developments that are helping municipal critical infrastructure owners and operators secure their systems from digital threats include:

- **Headway from the energy industry:** Regulatory standards for advancing cybersecurity have been implemented in the energy sector over recent years. This includes the NERC Critical Infrastructure Protection standards that are mandated in eight provinces, and the Ontario Energy Board's Cyber Security Framework.
- **Federal initiatives and tools:** The Government of Canada now offers two tools for critical infrastructure owners and operators to measure their cybersecurity postures, with plans to do more work on identifying municipal resilience needs.
- **Municipal councils prioritizing cybersecurity:** Support for cybersecurity initiatives by council members has been shown to vastly improve the cybersecurity maturity of municipalities.
- **Cyber insurance:** Qualifications for cyber insurance coverage have motivated municipalities to adopt better cybersecurity policies and practices.

In light of these findings, we offer five policy recommendations:

1. **Provincial mandates:** As the order of government with jurisdictional responsibility for municipalities, provinces should enact mandates and provide resources for local governments in their critical infrastructure cyber resiliency efforts. Different standards should be developed for different types of critical infrastructure at the provincial level (e.g., electricity, water, public transit).
2. **Cybersecure procurement:** In light of increasing supply chain attacks, infrastructure procurement practices and guidelines need to be updated to mitigate cybersecurity risks.
3. **Cybersecurity investment:** More dedicated funding for improving the cybersecurity of critical infrastructure is needed, including investments to enable municipalities to pay market rates for cybersecurity talent.
4. **Collaboration and information sharing:** Industry and all levels of government need to partner and share information on cyber threats and incidents in a more timely manner.
5. **Training for today and tomorrow's staff:** A culture of cybersecurity needs to be fostered across all organizational levels, with municipal management and councils at the forefront of supporting cybersecurity efforts. Addressing the widespread shortage of cybersecurity talent also requires training and reskilling programs.

Introduction



01

Introduction

> ***"We assess that, almost certainly, the most pressing threats to the physical safety of Canadians are to [operational technology] and critical infrastructure."***
>
> – Canadian Centre for Cyber Security (2020), National Cyber Threat Assessment 2020

Canada's economy, society and security rely on the uninterrupted functioning of our critical infrastructure. Critical infrastructure systems have been increasingly connected to information technologies, to improve process efficiency and service delivery. Despite these benefits, the connection of physical infrastructure systems to digital networks has made them more vulnerable to highly disruptive cyber attacks. With the growing adoption of smart systems and Internet of Things devices, it is essential that cybersecurity be embedded into critical infrastructure supply chains and asset management.

While critical infrastructure operators are grappling to protect their systems from cyber attacks, municipal critical infrastructure entities in particular face a unique set of challenges and limitations for addressing these issues. This project, supported by the Canada Infrastructure Bank (CIB) and Royal Bank of Canada (RBC), examines the challenges and opportunities for securing new and existing critical municipal infrastructure systems from cyber threats.

This report begins by laying out the array of cyber threats and resilience challenges to municipal critical infrastructure. What follows is a jurisdictional scan comparing the current state of provincial policies and guidelines related to cybersecurity for critical infrastructure. The paper then presents promising developments in the work to address the cybersecurity of Canada's new and existing municipal critical infrastructure; and concludes with a set of recommendations on how policymakers and partners can better support local governments in their efforts to protect their critical infrastructure from digital threats. This paper focuses on policy solutions; technical cybersecurity advice is out of scope of this report. This report is intended for federal and provincial policymakers, municipal councils, public and private sector investors, municipal critical infrastructure owners and operators, and those interested in advancing a cybersecure Canada.

Methodology

The focus of this paper is on critical infrastructure systems that are owned or operated by municipal governments in Canada. Our discussion of municipal **critical infrastructure (CI)** focuses on three particular sectors:

- Electricity and natural gas distribution systems;
- Drinking water, wastewater and stormwater systems; and
- Transportation systems (i.e., roads, public transit, airports).

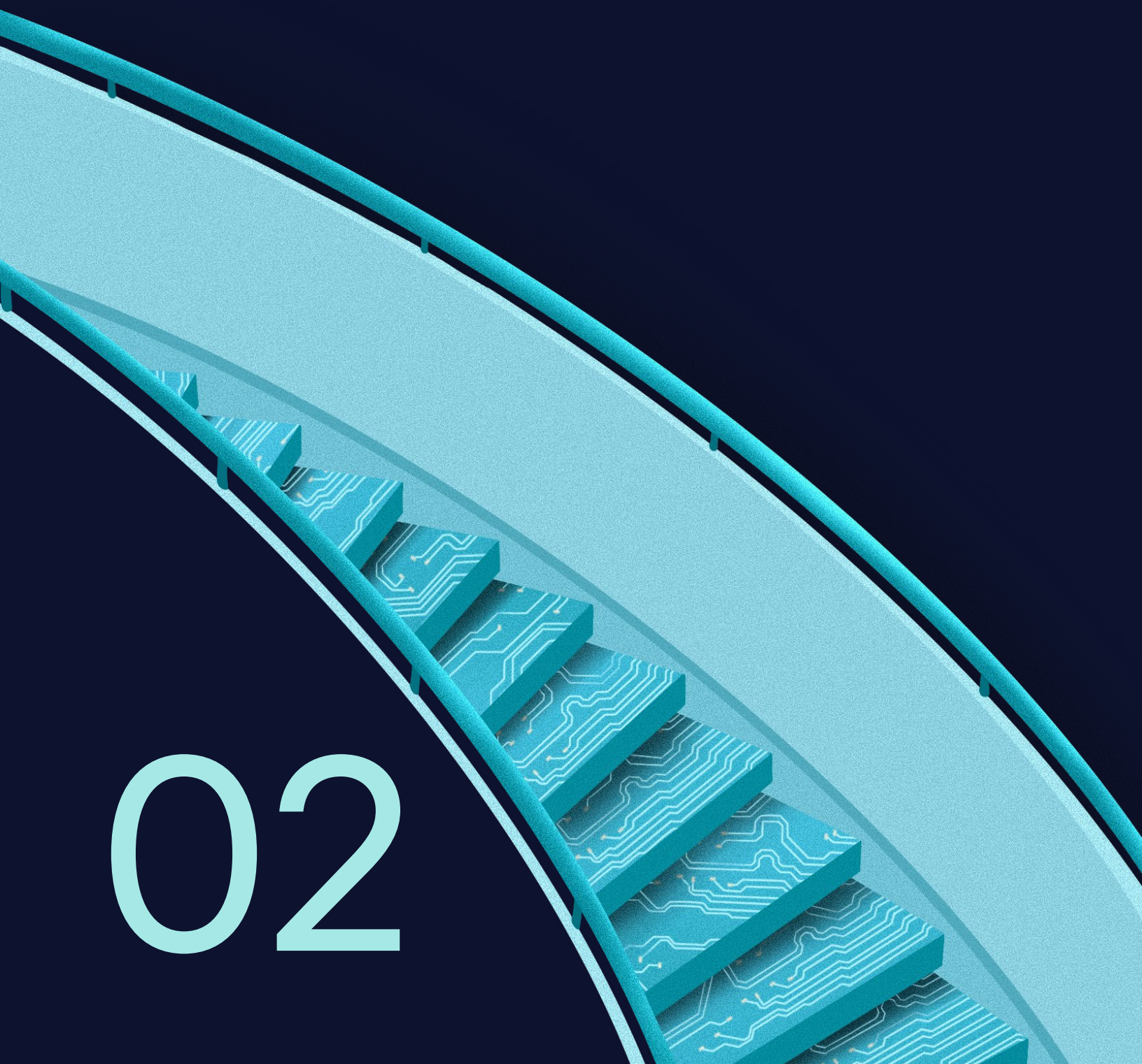
These CI systems were chosen because their operational technology — technology that controls physical processes — is increasingly connected to the internet.[1] **Operational technology (OT)** is used in CI systems to monitor and control processes and devices.[2] Connecting OT to the internet means physical systems are connecting to **Information Technology (IT)**.

The research that informs our findings and draft recommendations stem from:

- **A literature review** of the current state of understanding regarding municipal critical infrastructure resilience and cybersecurity.
- **A jurisdictional review** of all 10 Canadian provinces, to examine the presence of regulations and guidelines that aim to include cybersecurity considerations in critical infrastructure operations, emergency management, procurement and asset management.
- **Semi-structured interviews** and a **round-table** discussion with Canadian municipal leaders, municipal associations, infrastructure owners and investors, as well as engineering and cybersecurity industry professionals, to understand current perspectives, challenges and opportunities for securing networked municipal critical infrastructure. The round table was conducted under Chatham House Rule. The names of interviewees and municipalities are undisclosed at certain parts of the paper in order to protect confidentiality.

BACKGROUND:

Connecting Critical Infrastructure to the Internet



02

Connecting Critical Infrastructure to the Internet

> **Cyber resilience:** The ability of systems to maintain processes, operations, and data privacy and integrity in the face of targeted cyber attacks.

The Canadian government defines **critical infrastructure (CI)** as the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."[3] Canada has designated 10 infrastructure sectors as CI: energy and utilities, finance, food, transportation, government, information and communication technology (ICT), health, water, safety and manufacturing.

CI resilience is the capacity of a system to adapt and maintain an "acceptable level of functioning and structure" in the face of hazard exposure.[4] Resilient CI must be able to manage disturbances without loss of functionality, limited service interruption and efficient recovery time.[5] In this paper, we define **cyber resilience** as the ability of systems to maintain processes, operations, and data privacy and integrity in the face of targeted cyber attacks.

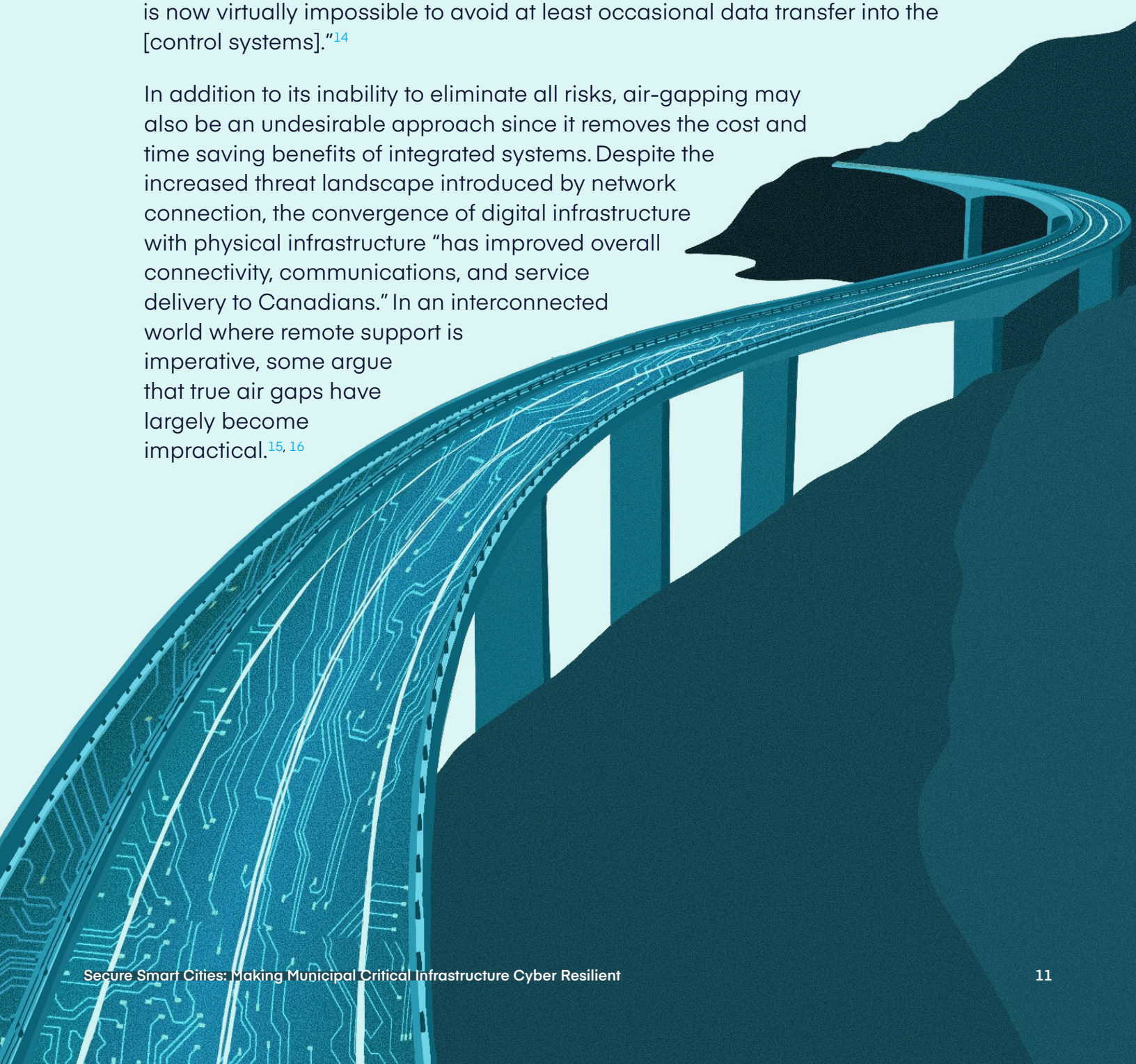
Connecting OT to the Internet

Infrastructure systems are increasingly connecting OT to IT in order to increase automation, enable remote monitoring, and increase efficiency. One set of OT, **Supervisory Control and Data Acquisition Systems (SCADA),** can remotely control processes, such as releasing water valves and initiating emergency shutdowns of systems.[6] Critical infrastructure industries that typically use SCADA include energy, water and transportation.[7, 8] SCADA devices and other similar systems were originally isolated from public networks, but have since become connected to the internet and other systems over time.[9, 10] Despite its benefits, the connection of operational technology to the internet has made SCADA-enabled critical infrastructure systems more vulnerable to cyber threats. According to Public Safety Canada, the use of internet-enabled systems by physical infrastructure "increases the probability and scale of both intentional and unintentional disruptions."[11]

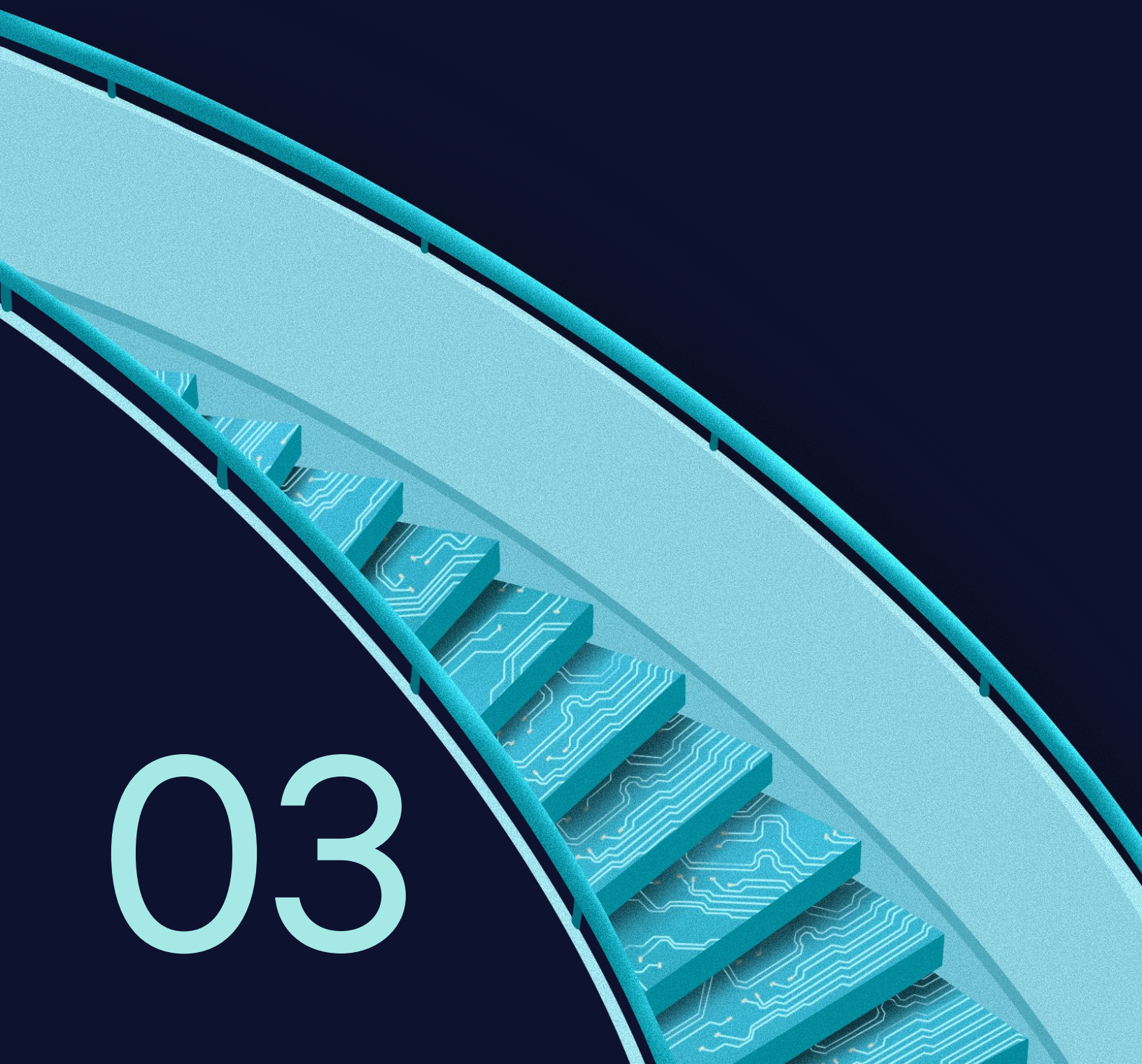
Can't risk be reduced by simply disconnecting critical systems from the internet?

An obvious approach to reduce risk is to simply disconnect CI systems from the internet. To "air gap" a system means isolating it from other systems or networks.[12] Although air-gapping a system protects it from fewer attack channels, it is not a foolproof way of securing infrastructure from cyber attacks for two reasons: first, systems that are isolated from other networks can still be breached;[13] and secondly, creating a true air gap is largely unfeasible as "it is now virtually impossible to avoid at least occasional data transfer into the [control systems]."[14]

In addition to its inability to eliminate all risks, air-gapping may also be an undesirable approach since it removes the cost and time saving benefits of integrated systems. Despite the increased threat landscape introduced by network connection, the convergence of digital infrastructure with physical infrastructure "has improved overall connectivity, communications, and service delivery to Canadians." In an interconnected world where remote support is imperative, some argue that true air gaps have largely become impractical.[15, 16]



Challenges to the cyber resilience of critical infrastructure



03

Challenges to the cyber resilience of critical infrastructure

Our research identified several key challenges faced by municipal CI owners and operators. These challenges include increased cyber attacks, infrastructure funding constraints and aging assets, and lack of provincial guidance.

Increasing cyber attacks targeting municipalities and CI

Operational technologies at the core of critical infrastructure face a wide range of cybersecurity threat vectors, including ransomware, phishing attacks, zero-day attacks, distributed-denial-of-service (DDoS) attacks and supply chain attacks.

Ransomware

Although ransomware attacks are not new, the scale, frequency and sophistication of ransomware attacks have dramatically increased to the point of becoming what the Canadian government has called "the foremost cyber threat facing Canadians and Canadian organizations."[17] Ransomware is a type of cyber attack where an adversary installs malicious software onto the target's system, typically locking and encrypting the device so that the victim organization cannot access its files until it sends a ransom payment.[18] This often occurs when a user within the organization accidentally downloads malware from an unknown source, usually through a phishing email that contains malicious links or attachments. Highly disruptive to an organization's operations, many organizations pay the ransom in order to regain access to critical files.[19] However, paying the ransom does not always guarantee regained access. In 2021, the majority of ransomware victims in Canada were critical infrastructure providers.[20]

Municipalities are highly sought-after targets for ransomware because their systems typically hold both large amounts of sensitive data pertaining to their residents, as well as connection to their infrastructure, such as water and traffic systems.[21] Without access to their data and systems, municipalities' operations, administration and service delivery can be highly disrupted. Desperate to restart operations, municipalities may give in to pressure to pay the ransom. This was the case for the City of Stratford in 2019, when they sent the equivalent of $75,000 in Bitcoin to their ransomware attacker in order to regain access to their systems.[22] The regional municipality of Mékinac in Quebec also paid a ransom to their attackers after a ransomware attack shut down their servers and left municipal employees locked out of their computers, paying a ransom in Bitcoin equal to $30,000.[23] Although the police advised the government to not pay the attackers, the region concluded that data re-entry efforts would be more costly than the ransom payment.

The 2021 **Colonial Pipeline** hack demonstrated the massive cascading impacts that ransomware attacks against CI can bring. Responsible for the largest fuel pipeline in the U.S., the ransomware attack led the Colonial Pipeline company to shut down their entire pipeline system in order to examine the extent to which their networks were compromised.[24] This led to higher fuel prices and gasoline shortages. The company ultimately paid their attackers $4.4 million in Bitcoin in order to regain access to their data, and to prevent their data from being leaked to the public.[25] The U.S. government's confidential assessment

reflected just how disruptive the cyber attack against the CI system could have been, concluding that "the country could only afford another three to five days with the Colonial Pipeline shut down before buses and other mass transit would have to limit operations because of a lack of diesel fuel. Chemical factories and refinery operations would also shut down because there would be no way to distribute what they produced."[26]

A ransomware attack disrupted Newfoundland and Labrador's health care system in October 2021, leading to the mass cancellation of medical procedures, including blood work and chemotherapy.[27] The personal information of patients and employees was also stolen from three regional health authorities,[28] including the social insurance numbers of over 2,500 patients.[29] Officials did not reveal whether a ransom was paid and also took several days to confirm a cyberattack had taken place.[30] That same month, a ransomware attack against the Toronto Transit Commission (TTC) led to the shutdown of several services, including their internal email system and their online booking system for accessible transit services for persons with disabilities.[31] It was unknown who the attackers were and whether any data were exfiltrated.

Supply chain attacks

Adding to the risk exposure and vulnerability of critical infrastructure are the complexity of supply chains and increase in supply chain attacks. Supply chain attacks involve compromising vendor systems, and their software or hardware products, in order to then compromise its customers.

Partly fueled by globalization and outsourcing, supply chains have grown in complexity over time,[32] in turn making it more difficult for organizations to identify and keep track of the security practices of their vendors.[33] Moreover, organizations with good cyber defences can still be vulnerable to supply chain attacks, as adversaries can infiltrate organizations by targeting their suppliers instead.[34]

Supply chain attacks are not new, but they are becoming more common for organizations including critical infrastructure operators. One survey of American and Canadian energy entities saw a 118% increase in reported supply chain incidents between 2019 and 2020, with 85 incidents reported in 2020 compared to 39 in 2019.[35]

One example of a major supply chain attack is the 2020 **SolarWinds hack**, which compromised an estimated 18,000 customers, including several critical infrastructure entities and agencies of the US government including the US Department of Energy's National Nuclear Security Administration.[36] After hackers installed malicious code into SolarWinds' Orion performance monitoring software, customers who then installed an Orion patch had backdoors installed on their systems.[37] These backdoors allowed attackers to access user networks and to transfer data from user systems. In what is likely a measure of security, the US government has yet to publicly identify which critical infrastructure entities were compromised by the hack.

Phishing attacks

Phishing attacks use websites, emails and other digital communications to trick the recipient into clicking a malicious link or downloading an infected attachment.[38] The attackers pose as trusted entities in order to install malware, such as ransomware, for the

purposes of identity theft, stealing funds or exposing sensitive data. These attacks have been reported since the 1990s, and are among the most widespread and common cyber attacks.[39]

Phishing allowed one of the dangerous malwares to be deployed onto the systems of a petrochemical facility in Saudi Arabia. Described as "the most dangerous threat activity publicly known," **Triton malware** was specifically designed to compromise industrial safety and control systems typically used in CI facilities.[40] In August 2017, a phishing attack facilitated the installation of the malware at the facility, after which attackers attempted to control the facility's industrial control system controllers. Fortunately, the facility intervened during the attack, preventing the malware from deploying its full functionality.

Phishing attacks rely on human emotions and common behaviours in order to achieve the attacker's desired outcome. One phishing attack in May 2019 left the City of Burlington with lost funds as a result of a phishing email. The phishing email was sent to the city's staff, requesting a change in banking information for a trusted vendor.[41] This led to an electronic transfer of funds totaling $503,000 to a falsified bank account.

Zero-day attacks

Although zero-day attacks and distributed-denial-of-service (DDoS) attacks are less of a CI cybersecurity concern compared to ransomware and phishing, these types of attacks have disrupted Canadian public services in the past.

When software has a security vulnerability, the developer can develop a security patch to fix it. An attack that exploits a security vulnerability before a patch has been developed is referred to as a zero-day attack ("zero-day" because the developers have already run out of time before the security flaw was exploited).[42]

In 2019, after discovering that their systems were infected by a zero-day virus, northeastern Ontario-based Health Sciences North shut down the IT systems of 24 hospitals within the region as a preventative measure to contain the virus.[43] The virus led to care interruptions, including slower services and temporary shutdown of their cancer program system.

DDoS attacks

A distributed denial-of-service (DDoS) attack targets websites, servers, online services or networks by overwhelming them with traffic in order to render them inoperable.[44] The main way these attacks are carried out is through a network of hacked computers or bots. Botnets (thousands to millions of controlled computers) are used by attackers to flood servers with a high level of traffic. DDoS attacks can sometimes include demands for ransom payments.[45]

In 2014, Hackers attempted to compromise the City of Orangeville's computer network through multiple DDoS attacks.[46] These attacks were aimed at the municipal network managing public Wi-Fi, phone systems and internet. The city's network was overloaded, rendering it unusable, but the town's firewalls were able to mitigate most of the attack.[47]

Constrained funding and aging infrastructure

Beyond digital threats, municipalities across Canada are continually struggling to fund the physical repair, replacement and protection of their CI assets. As the Saskatchewan Urban Municipalities Association (SUMA) put it, "municipalities collect approximately 10 cents of each Canadian tax dollar, but are responsible for nearly 60 percent of the public infrastructure."[48] Canada's infrastructure deficit is estimated to be between $150 billion to $1 trillion.[49] Climate change is further constraining infrastructure budgets, with municipalities requesting help from federal and provincial governments to fund climate mitigation and resilience projects to protect infrastructure.[50] Faced with challenges in funding the construction and maintenance of their infrastructure, municipalities are limited in their capacity to dedicate adequate resources to address cybersecurity risks.

- *"We know what we need to do and the programs we need to put into place, but we don't have enough resources and funding to do it."* **– Round table participant**
- *"The guidelines on how to do security are out there. The trick is to get the resources to do it."* **– Van Tran, City of Calgary**
- *"Municipalities are the layer that is closest to people's lives but ironically the most cash-strapped sector of government. This is the problem that needs to be solved. They need funding to define requirements, and additional funding to help them meet those requirements."* **– Omar Ahmed, Ipseity Security**

Legacy systems and aging infrastructure also pose serious risks to critical infrastructure cyber resiliency. Many legacy systems are still being used today in OT systems, and cyber threat actors will continue to target these aging or outdated systems until they are replaced.[51] Since these systems were not developed to withstand cyber threats, they can be particularly susceptible to attacks.[52] Rural municipalities are especially struggling to replace and update aging infrastructure due to a lack of funding and resources.[53]

In addition to existing infrastructure, weak attention to cybersecurity is also evident in plans for building new CI. We heard very little in our research engagements about how cybersecurity is explicitly addressed when planning new infrastructure projects. While utilities have recently implemented cybersecurity due diligence questionnaires for vendors, there is little indication that cybersecurity considerations or risks are considered or tracked throughout new infrastructure projects, particularly beyond the procurement stage.

Shortage of cybersecurity talent

The OT sector is facing a significant security labour shortage.[54] The industry is not alone, as 78 percent of Canadian IT managers report that their organizations are struggling to recruit and retain cybersecurity workers.[55] Interviewees emphasized the need for more cyber professionals in the field. Mark Fernandes, the Chief Information Officer of Hydro Ottawa, shared how resourcing has been a major challenge: "It's been hard to attract and retain cyber professionals, especially with competition in the market for the same resources."[56] Interviewees emphasized the need for more education and training to get more cyber professionals into the field.[57]

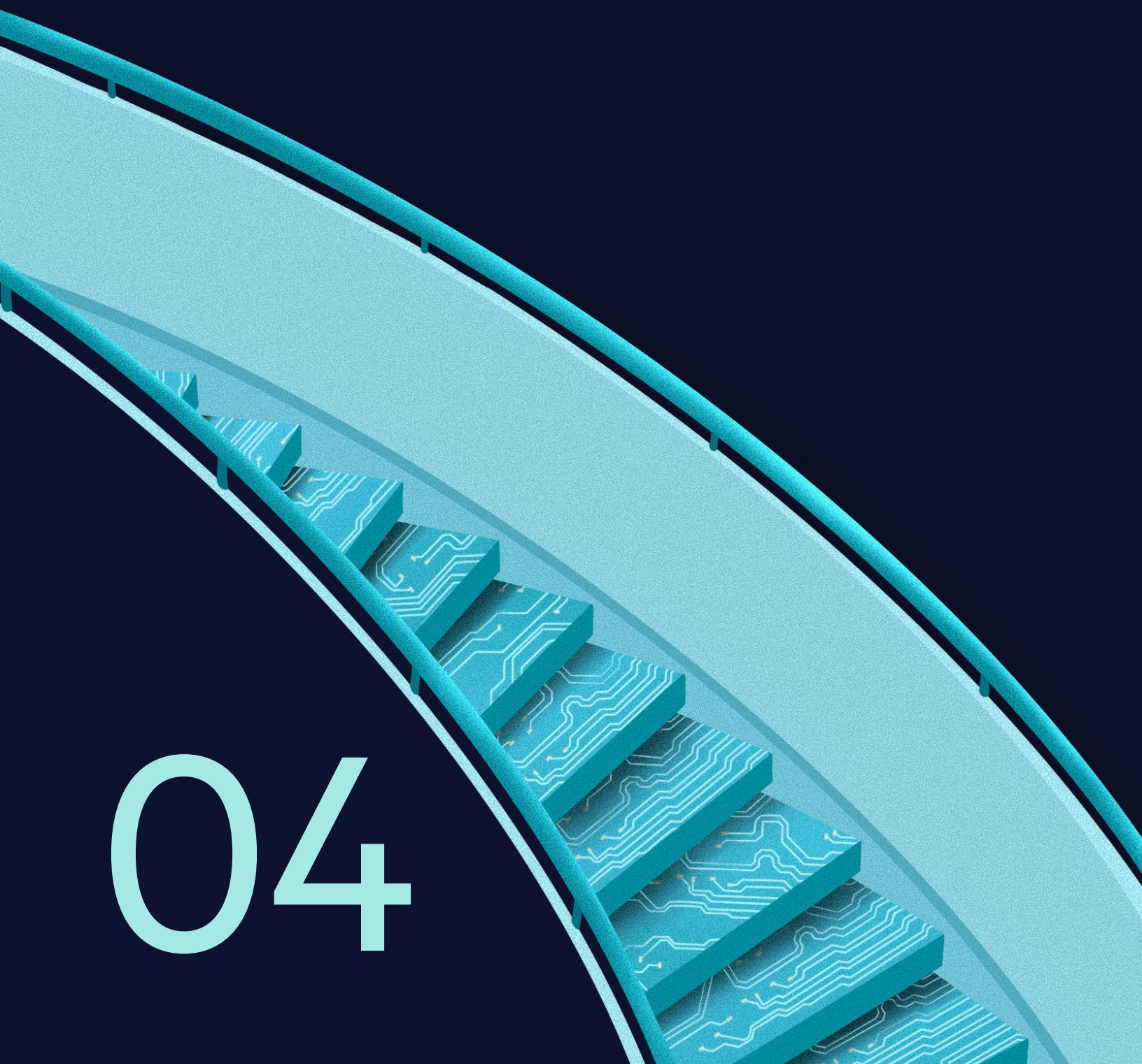
This shortage in IT talent is likely more acute in smaller, more rural municipalities. One interviewee shared how small and rural municipalities struggle to attract IT talent due to their size.[58] Another interviewee shared how capacities can be vastly different between different municipalities, which extends to their ability to hire and retain permanent IT workers.[59]

Cyber typically not covered in emergency management

Cyber-physical incidents occur when a cyber attack compromises physical systems, such as dams, pipelines and water treatment plants. These are becoming more common. Yet, as an emerging threat, municipalities are currently grappling with how cyber-physical emergencies should be planned for. With a traditional focus on physical disasters, emergency management structures tend to exclude cyber threats: "The concept of cyber security introduces complications to existing emergency management structures as cyberspace is independent of physical and geographical boundaries."[60] Cyber-physical incidents can leave teams unclear on who is responsible for responding, since IT teams are typically responsible for cyber incident response, and emergency management is responsible for physical emergencies.

Ownership over planning and execution of cyber-physical emergency management plans needs to be established by municipalities and provinces, as traditional emergency management structures may fail to meet the nuances of cyber-physical incidents. Jurisdictional authority should be clarified ahead of potential cyber-related incidents to CI. This includes the responsibilities of municipalities, the province, federal government and other accountabilities, such as police involvement.[61]

Scan of CI Cybersecurity Policies in Canadian Provinces



04

Scan of CI Cybersecurity Policies in Canadian Provinces

As constitutional authority for municipalities rests with Canadian provinces, the operations and asset management of municipal infrastructure is subject to various laws, policies and strategies established by provincial governments. We performed a jurisdictional review of the current state of provincial policies and guidelines related to cybersecurity for critical infrastructure, focusing on broad cybersecurity strategies and sector-specific guidelines, as well as emergency management, procurement and asset management policies that municipal infrastructure is subject to.

Province	Provincial cyber/ cybersecurity strategy mentions critical infrastructure?	Emergency management policy mentions cybersecurity?	Are there provincial cybersecurity regulations/ guidelines for energy suppliers?	Are there provincial cybersecurity regulations/ guidelines for water suppliers?	Procurement regulations/ requirements mention cybersecurity?	Asset management requirements/ guidelines mention cybersecurity?
Alberta	Yes	No	* Yes	Yes, under Guidelines for Municipal Waterworks (mandatory)	No	No
British Columbia	No	No	* Yes	No	No	No
Manitoba	No provincial cybersecurity strategy	No	* Yes	No	No	No
New Brunswick	No	No	* Yes	No	Plans to include cybersecurity in provincial procurement process	No
Newfoundland and Labrador	No provincial cybersecurity strategy	No	No	No	No	No
Nova Scotia	No	No	* Yes	No	No	No
Ontario	No	Yes, Ontario Hazard Identification and Risk Assessment Guidelines includes "cyber attack" under list of hazards to identify (voluntary)	* Yes. In addition to NERC standards, uses the Ontario Cyber Security Framework (mandatory)	Yes, Design Guidelines for Drinking-Water Systems (voluntary)	No	No
Prince Edward Island	No	No	No	No	No	No
Quebec	No provincial cybersecurity strategy	No	* Yes	No	No	No
Saskatchewan	No	No	* Yes	No	No	No
	1/10	1/10	8/10	2/10	1/10	0/10

** Mandated to follow NERC Critical Infrastructure Protection (CIP) standards, which includes cybersecurity requirements for critical infrastructure and assets.*

Provincial cybersecurity strategies

Provincial cybersecurity strategies are emerging, with seven out of ten provinces having released cyber or cybersecurity policies for protecting provincial systems at the time of writing. Out of these existing strategies, Alberta was the only province that mentioned protecting critical infrastructure from cyber threats. The Government of Alberta's Cybersecurity Services has adopted the industry-recognized National Institute of Standards and Technology (NIST) Cybersecurity Framework.[62] Alberta's Cybersecurity Strategy lists the NIST'S Cybersecurity Framework key functions, which includes developing and adopting appropriate protections for reliant critical infrastructure service delivery.[63] Despite this mentioning of critical infrastructure through the NIST framework, the province's Cybersecurity Strategy does not indicate any specific intention to address cybersecurity of CI systems within the province.

Emergency management

Comprehensive cybersecurity strategies encompass not only mitigation efforts, but also incident response and emergency preparedness. In Canada, provincial and territorial governments are responsible for emergency management within their jurisdictions.[64]

Cyber-related incidents were absent from all 10 provincial emergency management regulations. Ontario was the only province that included cybersecurity considerations in their emergency management guidance, which municipalities can choose to follow. The province's emergency management program provides resources to help municipalities conduct hazard identification and risk assessments. The Ontario Emergency Management Hazard Identification and Risk Assessment Guidelines includes cyber attacks as a hazard for municipalities to identify in their risk assessments.[65] The province's Hazard Identification Report provides constituents with more information on what cyber risks and cyber attacks encompass, defining cyber attacks as "an attack via cyberspace, for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[66]

Energy distributors

Our jurisdictional scan found that cybersecurity regulations for the energy sector were present in a majority of provinces (8 out of 10). This is largely due to regulations enforced by North America's largest regulator of energy distributors, the **North American Electric Reliability Corporation (NERC)**. The electricity sector in Canada and the U.S. largely follows the regulations and standards set by NERC, which are mandatory and enforceable in most provinces: British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, New Brunswick and Nova Scotia.[67, 68] NERC regulations include standards for identifying and mitigating cyber-related risks (more on these regulations can be found under Requirements-driven regulatory approach.)

In addition to NERC's regulations, the Province of Ontario has additional regulations for addressing the cybersecurity of energy CI systems. In 2018, the province's Transmission System Code was amended to require energy

transmitters and distributors to annually report cybersecurity readiness in reference to the Ontario Energy Board's Cyber Security Framework. Further discussion on this framework can be found under the section OEB's Cyber Security Framework.

NERC standards have not been formally adopted in the provinces of Newfoundland and Labrador, and Prince Edward Island (PEI). Newfoundland and Labrador Hydro has expressed intentions to voluntarily comply with NERC reliability standards.[69]

Water systems

Only Alberta and Ontario have included cybersecurity considerations in their water systems guidelines. Alberta's Guidelines for Municipal Waterworks lay out regulatory requirements for municipal system owners and operators of drinking water treatment, distribution and quality monitoring systems.[70] Section 2.7.4 focuses on securing SCADA systems and critical cyber assets "physically and logically" from unauthorized access and potential compromise.[71] The guidelines lay out practices for protecting SCADA systems, such as identifying all network connections on SCADA systems, configuring strong user authentication measures, installing and updating anti-virus applications, regularly updating patches to operating systems, and installing network logging and intrusion detection systems.

Ontario's Design Guidelines for Drinking-Water Systems is a voluntary framework for municipalities and owners of drinking-water systems.[72] It includes guidance on ensuring the reliability and security of systems, both physically and digitally. Its cybersecurity guidance includes selecting reliable software and hardware, local back-ups of system data, data encryption, and accessible vulnerability assessment documents. The guidelines emphasize that larger systems in the IT infrastructure be maintained through a security policy in order to prevent disruptions.

It is important for water suppliers to have cybersecurity regulations and guidelines due to the critical nature of water systems. A successful attack against water distribution and treatment systems can harm public health, the environment and economies, and lead to large-scale damage.[73] Cybersecurity must be leveraged in guidelines and regulations in order to manage the increasing risk that threat actors are imposing on water suppliers.

Procurement

Supply chain attacks are on the rise as attackers target organizations by compromising their software vendors (further discussed under Supply Chain Attacks). At the time of writing, no Canadian provinces include cybersecurity considerations in their procurement policies. New Brunswick's Digital New Brunswick Strategy mentions plans to embed cybersecurity within their standard procurement process,[74] although their updated procurement policy has yet to be released.

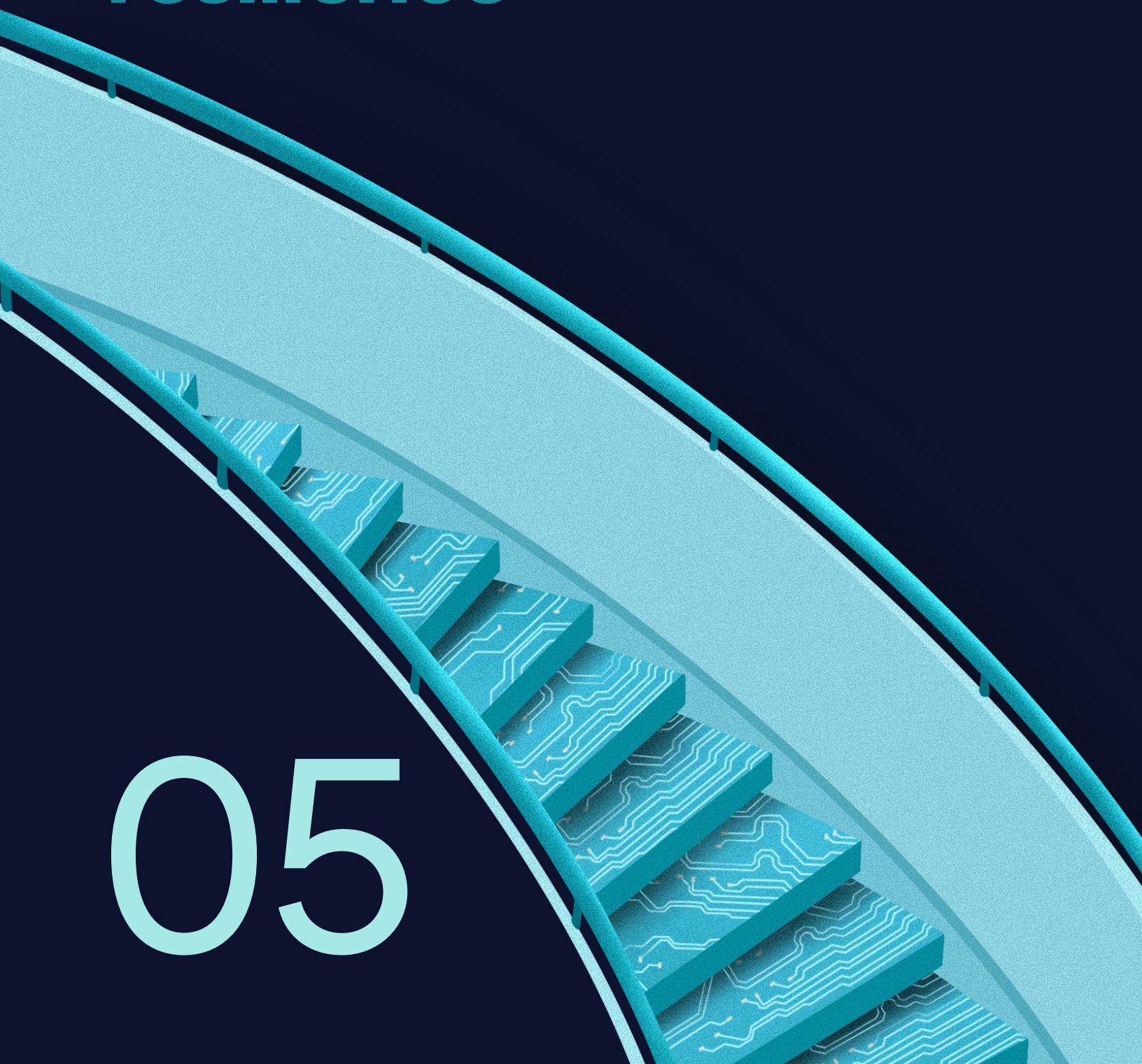
The absence of cybersecurity in provincial procurement guidelines is concerning, as it risks overlooking supplier risk during the procurement process. Compromises in the vendor's products and services can in turn leave public sector infrastructure and systems, such as digital transit fare and highway toll systems, vulnerable to cyber attacks.[75] With the growing adoption of smart systems and IoT, it is essential that cybersecurity be embedded into municipal and critical infrastructure supply chains.[76] In order to reduce cybersecurity risks, municipalities should map out their supply chain by determining a list of vendors, assess their supply chain through evaluation and accountability frameworks, assess cyber resiliency in procurement activities, review RFPs and vendor contracts, assess cyber insurance plans, and conduct cybersecurity assessments.[77]

Asset management

Asset management plans help municipalities monitor and manage their infrastructure assets in order to maintain service standards and reduce risks to operations.[78] Currently, there are no Canadian provinces that have asset management requirements or guidelines that mention cybersecurity.

It is integral that cybersecurity be considered in asset management plans to ensure cybersecurity risks are identified and addressed early. Proactively including cybersecurity measures is necessary to ensure that potential vulnerabilities are caught, and security threats are managed, before they create disruptions to service and potentially large-scale problems.[79]

Promising opportunities to increase cyber resilience



05

Promising opportunities to increase cyber resilience

Based on our literature scan and interviews, we've identified several promising developments that are helping municipal CI owners and operators secure their systems from digital threats. This includes the active policy leadership demonstrated by North America's largest energy regulator, federal initiatives for CI cyber resilience, support for cybersecurity initiatives by municipal councils, and the rise of cyber insurance.

Some early lessons from the energy sector

The regulations, programs and initiatives run by North America's largest energy distributor regulator serve as an example of the types of opportunities for making CI more resilient to digital threats.

Requirements-driven regulatory approach

The electricity sector in Canada and the U.S. largely follows the standards set by the North American Electric Reliability Corporation (NERC), including the **Critical Infrastructure Protection (CIP) reliability standards**. The standards aim to enhance the resilience of the Bulk Electric System from physical and digital security threats.[80] These standards are mandatory and enforceable in eight of Canada's provinces, requiring owners and operators of electrical CI to assess and mitigate cybersecurity risks.[81] CIP Cybersecurity standards include topics such as identifying and protecting cyber assets, disaster recovery planning, supply chain risk management, and more.[82]

OEB's Ontario Cyber Security Framework

The **Ontario Energy Board (OEB)** is the independent regulatory body of the province's electricity and gas sectors.[83] In 2016, the OEB convened a wide array of industry executives, experts and policymakers to develop a cybersecurity framework, the **Ontario Cyber Security Framework**. This framework provides a common basis for transmitters and distributors to assess their level of cybersecurity risk and maturity level.[84] The Framework also helps entities assess their compliance to privacy requirements set under federal privacy law and Privacy by Design principles. Since 2018, Ontario's energy transmitters and distributors are mandated under provincial legislation to report their cybersecurity maturity annually to the OEB using the Cyber Security Framework.[85] Recognizing the range of capacities, needs and maturity levels among infrastructure operators, Ontario's distributors are not required to comply with the Framework; instead, they are required to report how they measure against the framework, and set cybersecurity objectives depending on their level of risk.[86]

Interviewees from Ontario's energy industry shared praise for the impact that the Framework has had on the province's energy sector. One participant stated that, since the implementation of the Framework, Ontario's energy sector is now in a better state of readiness.[87] With the Framework leading to more awareness of cybersecurity risks and practices among energy distributors, "Ontario is a leader in the field of cybersecuring their electrical operations."[88] Another participant shared how the OEB Framework has improved the business case for organizations to properly invest in cybersecurity.[89] The annual reporting of energy distributors' Framework compliance

has encouraged energy entities to prioritize cybersecurity, while also providing regulators with insight on the cybersecurity postures of industry members.

However, there is still a lot more work that needs to be done to enhance the cyber resilience of Ontario's energy infrastructure. One round table participant felt that, despite the OEB mandate, the province's energy sector is still "blatantly behind and not up to speed" with managing cybersecurity-related risks. While noting that organizations are not required to fully comply with the Cyber Security Framework, the participant estimated that only a small portion of Ontario's energy sector organizations have fully met Framework standards.

Collaboration and information sharing

The OECD[90] and the U.S.' Cybersecurity and Infrastructure Security Agency (CISA)[91] emphasize that collaboration and information sharing between the government and infrastructure operators are necessary for fostering CI security and resilience. NERC's **Electric Information Sharing and Analysis Center (E-ISAC)** collaborates with Canadian and American government agencies to share timely security information to asset owners and operators. The E-ISAC acts as a valuable resource for its members and partners, providing resources, news, information-sharing programs, educational workshops, and more.[92] Last November, the E-ISAC convened over 700 utility owners, operators, and American and Canadian government officials, to host the largest grid security exercise in the continent.[93] The simulation tests the resilience of a bulk power grid against a major physical and cyber attack, giving participants the opportunity to connect and practice their emergency management skills.

Federal initiatives for CI cyber resilience

The Government of Canada has been taking steps to assist CI owners and operators in ensuring the cybersecurity resiliency of their systems, with forthcoming plans to identify ways to better support municipal CI. Public Safety Canada currently provides two different cybersecurity and infrastructure resilience assessments for critical infrastructure owners and operators. The first is the **Canadian Cyber Security Tool (CCST)** — a voluntary self-assessment that CI entities can undertake to review their operational resilience and cybersecurity maturity.[94] After completing the self-assessment, participants receive a report with guidance on how to improve their cybersecurity resilience. Post-self-assessment results also show participants how their cybersecurity posture compares to others within their sector. Designed to be quick and easy, the CCST takes about an hour to complete.[95] One interviewee complimented the CCST, finding it to be really helpful for municipalities to benchmark themselves against their peers.[96]

Public Safety Canada also offers a more comprehensive resilience assessment under the **Regional Resilience Assessment Program (RRAP)**. RRAP consists of free and voluntary on-site assessments that take at least four days to complete.[97] While the RRAP offers a thorough assessment and detailed guidance on improving physical and cyber CI resiliency, the bar is higher for accessing this program compared to the CCST, as CI owners and operators must first be accepted by Public Safety Canada to participate in the program.

Looking ahead, the Government of Canada is in the process of developing the National Infrastructure Assessment. The Government's envisioning of the assessment includes examining cyber threats and cyber resilience of infrastructure.[98]

Need for clear communication resources

Federal initiatives like these may not be on the radar for many municipalities. Several round table experts and interviewees noted a lack of communication to municipalities regarding the cyber resilience resources, programs and guidance available to them. Annalise Czerny, public sector consultant and former Chief of PRESTO for Metrolinx, shared how "Clear communication of resources ([such as] groups, information about standards, etc.) is needed. It was fortunate in our case that we found out that there were federal resources we could tap into. I always wondered: why wasn't everyone aware?"[99]

Municipal councils prioritizing cybersecurity

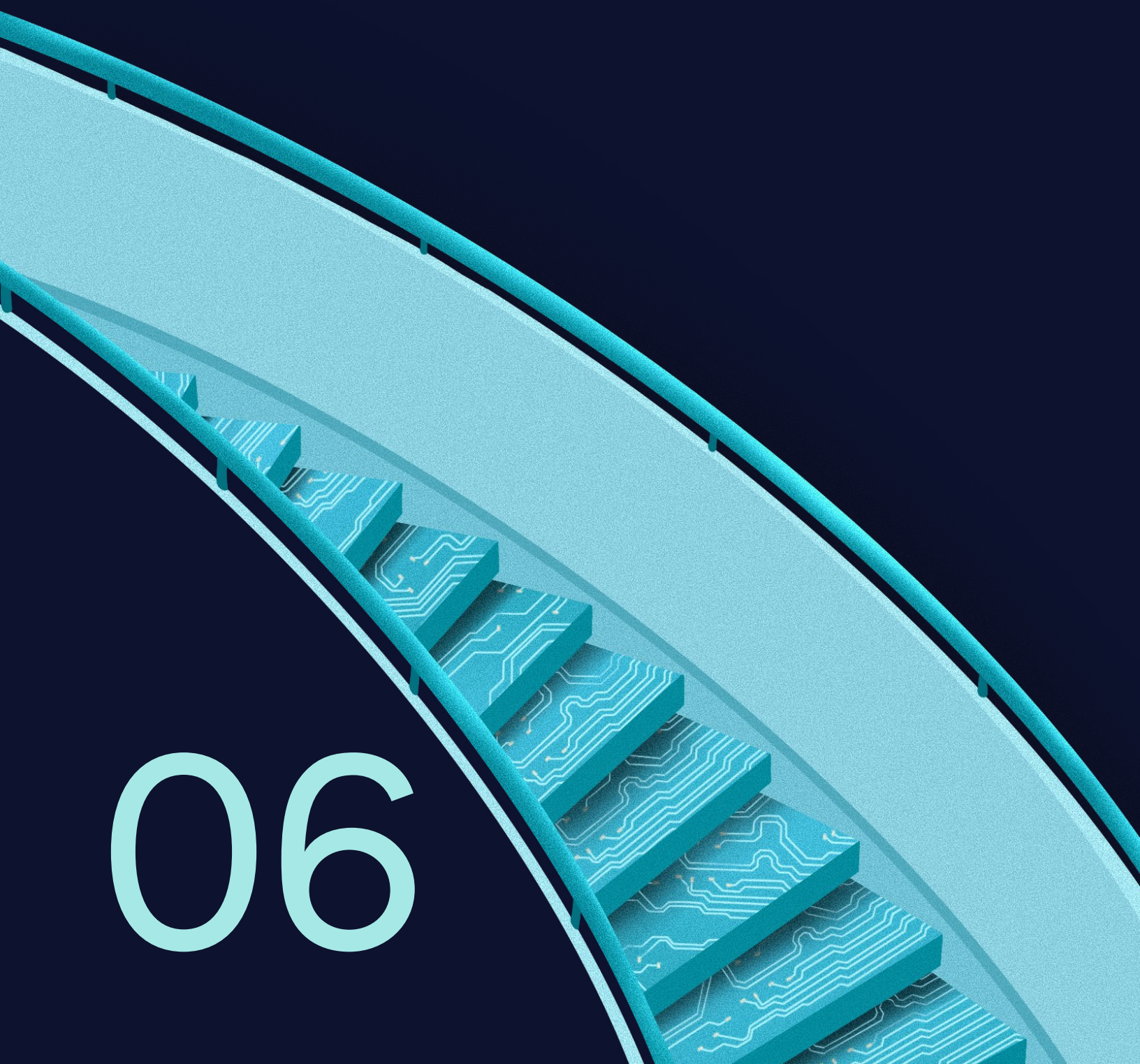
Prioritization of cybersecurity varies between municipalities, with interviewees sharing that a lack of awareness among municipal leadership usually leads to low support for cybersecurity work or investments. One interviewee shared how they have struggled over the years to get approval from council for necessary cybersecurity resources for protecting their CI systems: "It's really concerning trying to change the mindset for upper management. It's like being proactive with safety: people don't want to pay unless something happens."[100]

While some municipal staff are struggling to get their council's attention on cybersecurity needs, others have been able to adopt strong cybersecurity policies as a result of supportive council leadership. Ryan Sorrey, the Chief Information Officer for the City of Moncton, shared how support from his city council has allowed the municipality to actively build cybersecurity capacity for over a decade.[101] Such support has enabled funding for cybersecurity-enhancing programs and activities, such as system penetration tests. Dave Schultz, Security Manager for the City of Lethbridge's Information Technology Services and Digital Transformation department also shared how city council support helped advance the municipality's cybersecurity. Several years ago, the council approved a cybersecurity initiative that centralized the organization's cybersecurity services and hired permanent IT security staff.[102] Council support also enabled the development of the city's vulnerability management program, which helps staff identify and mitigate cybersecurity risks.[103]

Cyber insurance

Across Canada, municipal governments are purchasing cyber insurance coverage to cover potential losses from a cyber attack.[104] Cyber insurance coverage has become increasingly appealing to municipalities as ransomware incidents rise. However, to qualify for cyber insurance, organizations must have adequate cybersecurity and data governance procedures in place. This has resulted in some municipalities adopting better cybersecurity practices and policies to meet the standards necessary for cyber insurance coverage, or to apply stricter standards to seek lower premiums. These requirements set by cyber insurance companies have motivated municipalities to adopt better cybersecurity practices – a promising development for improving the cybersecurity of municipal and CI systems.

Policy Recommendations



06

Policy Recommendations

Based on the research findings, interviews and round-table discussions, policy recommendations have been developed for municipalities, federal and provincial governments, municipal critical infrastructure owners and operators, public and private infrastructure investors, municipal associations, and other relevant stakeholders.

1. Provincial mandates

Provinces have a major role to play in advancing the cyber resilience of the municipal CI systems in their jurisdictions, particularly in sectors such as municipal water, energy and transportation that are regulated by provincial/territorial governments.

Regulations should be implemented by provinces and territories that require municipalities to put cyber resilience measures in place for CI. They should be designed to recognize that capacities and risk profiles differ among local governments.

One approach for advancing municipal CI cyber resiliency is requiring CI owners and operators to annually report on their cybersecurity posture using provincial, industry-consulted cybersecurity frameworks to assess their cybersecurity risks and maturity. Frameworks should be collaboratively developed for specific municipal CI sector types such as water and transportation. Similar to the Ontario Cyber Security Framework, these frameworks should include a methodology for CI entities to assess their cybersecurity risk level, and a self-assessment tool to gauge the organization's level of compliance to cybersecurity and privacy principles.

Developing these guidelines at the provincial level can be beneficial since it can provide more clarity for municipalities on their province's responsibilities, resources and relevant legislation. Enacting mandatory reporting also improves the business case for municipalities to invest in cybersecurity. Another benefit of creating cyber resiliency frameworks is, as existing industry standard frameworks can be numerous and extensive, municipalities may struggle to determine what their first step should be.[105] Provincially-developed guidelines can clearly synthesize these industry frameworks, allowing local governments to get a better handle on their action plan.

This approach encourages annual cybersecurity risk assessments, which are key to the development of a comprehensive cybersecurity strategy, since they can be used by municipalities to identify security gaps and strategies for improvement.[106] However, as several interviewees pointed out, traditional risk assessments can be a very expensive exercise. The ability to conduct risk assessments can depend on an organization's staff and capacity, and the managers' ability to inform councils and mayors.[107] One interviewee recommended that a risk assessment model be developed that is more rapid, targeted and specifically geared toward specific infrastructure sectors.[108] Considering the high cost of risk assessments, and the different capacity levels among municipalities, federal and provincial funding should be provided to facilitate these initiatives.

Balancing Regulations: Notes from our Round Table

Round table participants largely agreed that provincial regulations are necessary for nudging municipal CI owners and operators into prioritizing CI cyber resilience. A participant commented: "Without regulation, what to do, how much to do, and how much funding to dedicate becomes a risk decision that can be prioritized or de-prioritized." Another participant similarly noted that: "Regulation elevates the decision. It becomes a council and executive leadership conversation. That leads down to the right path."

Avoid overwhelming requirements

At the same time, several round table participants noted that newly-introduced mandates need to be mindful of overwhelming municipalities:

- *"If you want people to engage in this work and provide that standard, you also have to be careful about not being overbearing."*
- *"You don't want to overwhelm people with a thousand things to do. Start with critical controls that need to be put in place and then over time step it up."*
- *"Let's start with a few things to get municipalities to 80%, that way it's less daunting."*

Accountability mechanisms

Effective regulation in this area also necessitates ways to ensure accountability of municipalities, and transparency of policy progress:

- *"Frameworks and guidelines are nice, but if there are no teeth behind it then what moves the needle?"*
- *"Until there are significant enough consequences to non-compliant organizations, they will look at guidance as only that."*
- *"As regulation is being developed, who do we make responsible for those mechanisms?"*

Data governance alongside cybersecurity

The need to include data governance and privacy in municipal and CI cybersecurity policies was also emphasized by round table participants and interviewees. This is especially fitting, as sensitive data on OT systems can be used by adversaries to design their cyber attacks.[109]

- *"Need to consider that it is also Data Governance programs in addition to cybersecurity. Stronger data governance works hand in hand with cybersecurity. Nearly no cities in Ontario have Data Governance programs in place. This is critical for the protection of personal information, and data classification. Ultimately, this will have a significant outcome on ensuring cybersecurity insurance."*
- *"The need for data security is the same regardless of population size."*
- *"I think municipalities aren't thinking beyond the physical road. They aren't thinking about the data collected, which is susceptible to attack because they don't understand what they need to be guarding in the first place."*[110]

Municipal CI owners and operators also need clarification on their responsibilities; the responsibilities of the province and relevant bodies; and the options and resources that are available to them. Since CI sectors are regulated by different ministries and standards, sector-specific guidance is required. A good example of the structure that guiding documents can take is the Association of Municipalities of Ontario (AMO)'s Municipal Cyber Security Toolkit.[111] Although the toolkit only pertains to municipal cybersecurity in general, it provides municipalities with guidance on the roles of the provincial government, police services and municipal associations regarding municipal cybersecurity. The resource clearly lays out the range of considerations and options for municipalities in improving their cybersecurity readiness in a variety of areas, such as audit considerations, insurance considerations, and IT policies and procedures.

One round table participant noted how the prevention of cybersecurity incidents is not enough; organizations need to have guidance on the appropriate actions to take during cyber attacks in order to minimize the severity of impact. This includes clarifying which groups to report to and when; and what bodies have jurisdictional authority when it comes to reporting and investigating cyber threats and attacks. As one participant noted, "You don't want to figure out those questions in the middle of a crisis."[112] Two interviewees mentioned the need for provincial guidance on how municipalities should manage communications and public messaging during cyber attacks.[113]

2. Cybersecure procurement

> ***"The tendering process has to be shaped to ensure protection."***
> – Ryan Sorrey, CIO and Director of Information Systems at City of Moncton

With the increasing frequency of supply chain attacks, municipal and provincial procurement guidelines need to be updated to mitigate cybersecurity risks.

The European Union Agency for Cybersecurity recommends that organizations practice due diligence when selecting and validating their vendors.[114] The SANS Institute's 2021 survey found that a majority of OT industry members (71% of respondents) consider pre-qualifying vendors and their cybersecurity postures as either mandatory or highly important.[115] There are a few immediate opportunities for embedding cyber resilience in procurement policies.

i) Building a directory of vendors vetted for cyber resilience

While assessing the cybersecurity maturity levels and practices of technology vendors is a necessary measure for mitigating the risk of third-party attacks, some municipalities may lack the capacity and resources to thoroughly assess each potential vendor. One potential measure for more cybersecure procurement would be the development of a directory of vendors whose cybersecurity posture has been reviewed and approved by trusted entities, such as municipal associations or provincial bodies. Local governments can then refer to this directory when selecting vendors. This

approach allows municipalities and related bodies to collaborate on vetting suppliers, rather than working and dedicating resources in independent silos.

ii) Establishing shared service agreements for affordable cybersecurity services

Another collaborative and potentially cost-saving measure would be developing shared service agreements between municipalities for IT and cybersecurity services. Securing a volume discount rate can make it more feasible for resource-strapped municipalities to procure IT and cybersecurity resources. An example of this is the Alberta Urban Municipalities Association (AUMA)'s partnership with Canadian cybersecurity-as-a-service company, Stratejm. After negotiating with Stratejm, AUMA and Stratejm developed an arrangement that provides AUMA's municipal members with volume discounts on Stratejm's cybersecurity services, making "cybersecurity more affordable to individual municipalities."[116]

iii) Adding cybersecurity clauses to tendering documents

Including cybersecurity requirements in every Request for Proposal (RFP) and contract is another measure that can help mitigate risks.[117] This includes security standards, security terms and conditions, and ways to ensure follow-through of security agreements. NIST's *Best Practices in Cyber Supply Chain Risk Management* highlights that utility organizations should be afforded audit rights to review vendor compliance to contractual agreements.[118] Such cybersecurity clauses should be included in all RFPs and contracts pertaining to existing CI systems, as well as infrastructure that is planned to be developed.

Some interviewees shared how their municipalities have already been incorporating cybersecurity clauses into their RFPs. These clauses state that vendors must follow industry cybersecurity standards, with some instances requiring proof of credentials, such as relevant cloud security certifications. Igor Zaslavsky, York Region's Manager of Transit Management Systems, shared how suppliers have become increasingly upfront about their cybersecurity practices: "It's a shift where vendors understand the importance of cybersecurity. They provide a lot more information now on how secure their systems are and what cybersecurity measures they have in place."[119]

However, a few round table participants expressed hesitation regarding overly prescriptive cybersecurity clauses that result in few if any vendors bidding. One participant noted that smaller organizations would benefit more from having vendors precleared through a central entity rather than enforcing cybersecurity requirements that are too specific.

3. Cybersecurity investment

New and sustainable investment schemes are needed to support municipal CI owners and operators in their cybersecurity efforts.

Investments in resilient infrastructure are critical and cost-saving. Investors that make resilient infrastructure investments see a return of investment of $6 in future averted losses for every $1 spent proactively.[120] Investing to ensure the uninterrupted functioning of CI can offset costs that result from security breaches, such as infrastructure disruption, system recovery, data recovery, fines and litigation.[121]

With growing costs associated with adapting to the impacts of climate change and replacing aging infrastructure, the budgets of CI owners and operators are especially stretched to address simultaneous major threats to system resiliency. To ensure that cybersecurity gets the investment and attention that it requires, federal and provincial funding programs should be established to specifically support municipalities in CI cyber resilience work. Development of public and private sector investment partnerships can help further boost funding in this area.

Investments also need to be sustainable. Regarding the increased risk to Canadians' physical safety as a result of internet-connected OT devices, the Canadian Centre for Cyber Security states how "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." Municipal CI owners and operators require sustainable investments to help ensure that cybersecurity maturity can be maintained over time.

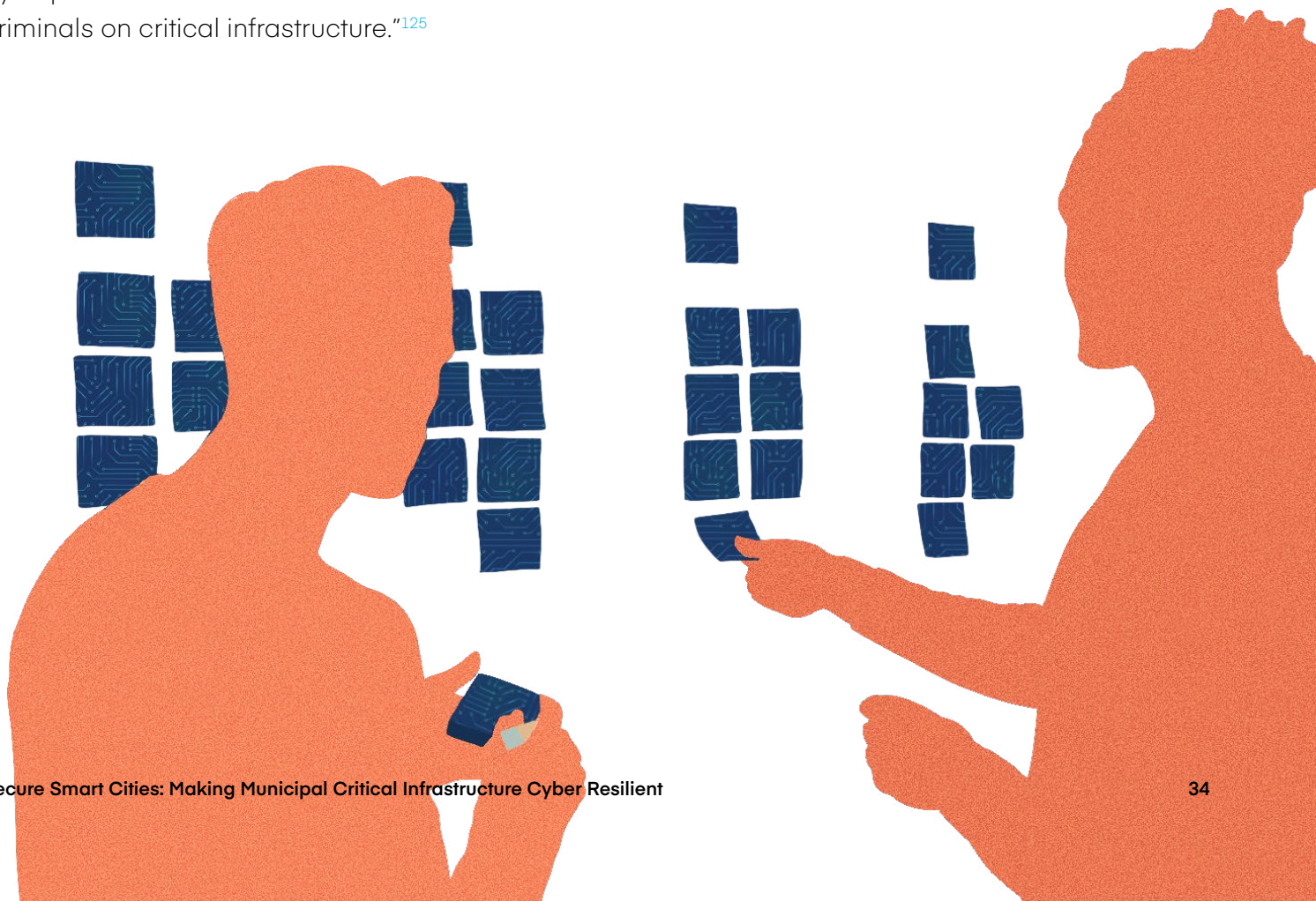
At the same time, the market for cybersecurity talent is extremely competitive amidst a nation-wide shortage in cybersecurity professionals.[122] In order to attain and retain cyber experts, municipalities will have to pay market rate for this expertise, which requires further investment.

4. Collaboration and information sharing

Information on security threats, incidents and lessons learned should be more accessible for municipal CI entities.

Although Canada's National Strategy recognizes the significance of cooperation and information sharing between governments and CI owners and operators for CI resilience,[123] more work needs to be done in this area. The Canadian Electricity Association urged the Government of Canada to increase its intelligence sharing on security threats to the grid "in even more timely and actionable ways."[124] NERC similarly recommended in their 2021 State of Reliability report that industry and government "should significantly increase the speed and detail of cyber and physical security threat information sharing in order to counter the increasingly complex and targeted attacks by capable nation-state adversaries and criminals on critical infrastructure."[125]

National data on cyber incidents among CI sectors and municipalities should also be available for organizations. One interviewee shared how such data would be helpful for conveying the seriousness of cyber attacks to management. Research participants also noted that information on municipal cyber incidents would be informative and helpful for supporting the business case for cybersecurity work: "There is a big struggle in getting municipalities to share attacks that occur. We need to share this information so people understand the priority it has. Maybe that's why heat isn't being put on industry – because no one wants to talk about it."[126]



5. Training for today and tomorrow's staff

Aside from the technical aspects of cybersecurity, the human side of the issue needs to be addressed through continuously updated training for municipal employees at all levels.

i) Fostering a culture of cybersecurity across all levels

Ongoing cybersecurity awareness training should be a requirement of municipalities for their staff and council. Phishing scams, ransomware and other cyber incidents can be avoided when municipal staff and council members are trained to recognize cybersecurity risks. The constant evolution of cyber threats necessitates a culture of cybersecurity awareness.[127] Developing this culture requires mandatory, continuous and appropriate cybersecurity education for all staff throughout their employment with the municipality. Council members and senior municipal staff have an important role to play in this work since they "are uniquely placed to promote a culture of awareness and prevention, and ensure that vulnerabilities are assessed, cyber security plans are established and accountability measures are put in place."[128] As one interviewee put it, "human resources may be even more important than the technology side."[129]

Round table participants also noted that a healthy cybersecurity culture requires a reshifting of the incentives structure for municipal IT directors: "The rewards structure for IT directors must change. They get rewarded for the number of systems they deliver, being on budget, operations up time… but how many IT directors get rewarded on data governance, cybersecurity practices, policies, data handling?" Providing recognition for IT directors for their cybersecurity work can be one component for improving organizational culture.

> ***"The least expensive approach to effective cyber security is emphasizing education and training processes on people. Post data breach is more expensive than pre data breach and municipalities should be considering hardening not just their technology and systems but their people as well."***
>
> – Association of Municipalities Ontario. (2020). *A Municipal Cyber Security Toolkit: Best Practices to Guide and Improve Cyber Security Readiness*

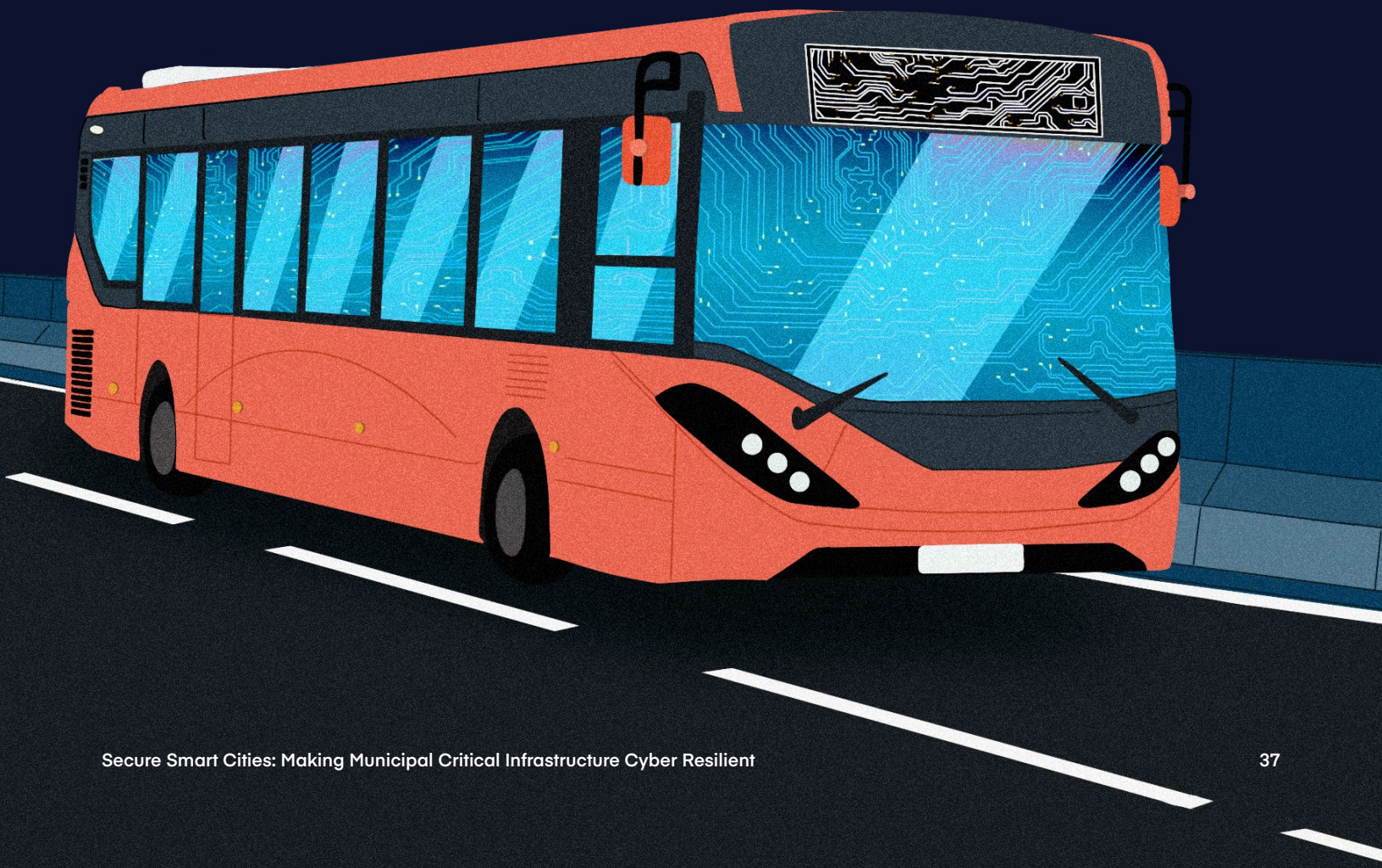
Cybersecurity training, education and awareness is also necessary for municipal leadership to better prioritize and delegate resources for cybersecurity efforts. Councils that are aware of cybersecurity risks are more likely to support the development and implementation of cybersecurity initiatives and programs. In order to facilitate council support, senior management, directors and CIOs need to drive the importance of cybersecurity to their councils. For one interviewee's municipality, this meant adopting practices to ensure that cybersecurity updates were reaching the top of the organization: "Our cybersecurity scans go to the top. Cybersecurity updates go to the managers. Senior management then writes the report to the council to request funds. This didn't happen overnight – it was part of lessons learned."[130]

ii) Training programs for future talent

In this competitive market for cybersecurity talent, it is difficult for smaller municipalities and utilities to compete for IT resources. Addressing the talent shortage requires investments for training and reskilling programs in order to fill this gap in human resources. Another option for harnessing future talent could be through provinces centralizing a co-op program for cybersecurity students to become partnered with municipalities.

Conclusion

Today's municipal critical infrastructure systems need to be resilient – not just to physical threats, but to digital threats as well. The Colonial Pipeline hack showed the level of disruption that a successful cyber attack can unleash. We must ensure that municipally-owned or operated critical infrastructure systems are able to withstand increasingly sophisticated and frequent digital threats. Municipalities, the federal and provincial/territorial governments, and many other stakeholders, all have a role to play in addressing this issue. With the necessary investment, human resources, guidance and regulation, municipal critical infrastructure can reach the cybersecurity posture needed to be resilient against evolving digital threats.



About the Authors

Stephanie Tran is an experienced researcher with over five years of experience analyzing public policy and human rights issues related to digital technologies, with past experience working for the Citizen Lab, Amnesty International Canada, the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) and more. She is a trained computer programmer, having earned a Diploma in Computer Programming from Seneca College. She also holds a dual degree Master of Public Policy (Digital, New Technology and Public Affairs Policy stream) from Sciences Po in Paris, and a Master of Global Affairs from the University of Toronto. She earned her BA degree from the University of Toronto specializing in Peace, Conflict and Justice.

Sharan Khela is a Master's of Public Policy and Administration student at Ryerson University. She holds a BAH in Criminal Justice & Public Policy with a minor in Philosophy from the University of Guelph. Her research experiences include working as a Research Coordinator for Laadliyan, Advisory Committee Member for the Youth Secretariat's State of Youth report, and as a Research Associate for an EDI and Anti-Racism consultant where she worked on a contract for the Ontario Council of Agencies Serving Immigrants (OCASI). Sharan is passionate about community building, youth development and advocating for marginalized immigrant communities.

André Côté has worked in a variety of roles at the intersection of higher education and tech. As mission-driven consultant, offer strategic advice, research and other services to a range of clients. As senior advisor to Ontario's deputy premier and minister of advanced education and skills development, and for digital government services. As chief operating & strategy officer with NEXT Canada, a national non-profit incubator for entrepreneurs and start-ups. As ed tech innovator, developing the Dive: Student Aid digital case learning model with RLL and other partners. And as a director on the Board of eCampus Ontario. He's published many papers, reports and articles, including in other past roles with IMFG, a cities-focused research institute at the University of Toronto's Munk School of Global Affairs and Public Policy; and with the Public Policy Forum. He is a graduate of the Munk School's Master of Public Policy (MPP) program, and Queen's University.

Appendix A: Interviewees and Round Table Participants

We are immensely grateful for all the interviewees and round-table experts who generously shared their time and expertise for this report.

Withstanding privacy and security, some names and affiliations have been withheld.

1. **Adam Evans,** Royal Bank of Canada (RBC)
2. **Andrew Posluns,** Canada Infrastructure Bank
3. **Andy Best,** Civic Digital
4. **Annalise Czerny,** Annalise Czerny Consulting Inc.
5. **Chris White,** ERTH Corporation
6. **Connie McCutcheon,** MISA Canada
7. **Craig Pettigrew,** Rural Municipalities of Alberta (RMA)
8. **Daniela Spagnuolo,** Association of Municipalities of Ontario
9. **Dave Colvin,** Ontario Association of Emergency Managers (OAEM)
10. **Dave Schultz,** City of Lethbridge
11. **David Williams,** ERTH Corporation
12. **Glenn Miller,** Canadian Urban Institute
13. **Greg Markell,** Ridge Canada Cyber Solutions Inc.
14. **Hamish Goodwin,** City of Toronto
15. **Hani Mansi,** City of Edmonton
16. **Igor Zaslavsky,** York Region
17. **Jason Besner,** Canadian Centre for Cyber Security
18. **Jay Meyer,** Saskatchewan Association of Rural Municipalities (SARM)
19. **Jean-Marc Nadeau,** Saskatchewan Urban Municipalities Association (SUMA)
20. **Katherine Kolnhofer,** Bell Temple LLP
21. **Konrad Siu,** University of British Columbia
22. **Kush M Sharma,** MISA Ontario
23. **Lacey Barnhard,** Rural Municipalities of Alberta (RMA)
24. **Laurie Palmer,** ERTH Corporation
25. **Mark Fernandes,** Hydro Ottawa
26. **Nabeel Ahmed,** City of Toronto
27. **Omar Ahmed,** Ipseity Security
28. **Ryan Sorrey,** MISA Atlantic
29. **Sarah Teal,** Mariner Innovations
30. **Steve Czajka,** Data Professional
31. **Van Tran, City of Calgary,** Water Utilities
32. **Wally Wells,** Asset Management BC
33. **Zachary Spicer,** York University's School of Public Policy and Administration

Appendix B: Available Cybersecurity Guidance for Municipalities

Association of Municipalities Ontario. (2020). A Municipal Cyber Security Toolkit: Best Practices to Guide and Improve Cyber Security Readiness (p. 23). Association of Municipalities Ontario.

https://www.amo.on.ca/sites/default/files/assets/DOCUMENTS/Reports/2020/AMunicipalCyberSecurityToolkit20200930.pdf

Discusses the cybersecurity needs of Ontario municipalities and explains why municipalities are targeted by cyber attacks. Provides a range of cybersecurity advice for municipalities, including insight on Cyber Security Risk Assessments, incident response planning, security protocols, and more.

Miller, G. (2021, June 22). Prepare For the Worst, Hope For the Best. ReNew Canada.

https://www.renewcanada.net/feature/prepare-for-the-worst-hope-for-the-best

Article synthesizes the available expert advice on ensuring the cybersecurity of Canadian municipal critical infrastructure (based on AMO, Ontario's Cyber Security Centre of Excellence, CyberNB and the Cyber Centre). Provides an overview of the municipal critical infrastructure cybersecurity work being done in Alberta with AUMA, and in Ontario with AMO's Digital Government Taskforce.

Internet Society & Next Century Cities. (2019, November 1). Security Factsheet: Why Should Municipalities Make Network and Data Security a Priority? Internet Society.

https://www.internetsociety.org/resources/doc/2019/why-should-municipalities-make-network-and-data-security-a-priority/

Factsheet intended for municipalities seeking to minimize their cybersecurity risks. Provides cybersecurity practices for local governments, such as setting strong internal data and security policies.

Canadian Centre for Cyber Security. (2018). State-Sponsored Espionage and Threats to Critical Infrastructure. Canadian Centre for Cyber Security.

https://www.cyber.gc.ca/en/guidance/state-sponsored-espionage-and-threats-critical-infrastructure

Outlines types of critical infrastructure sectors; why critical infrastructure is an attractive target for espionage by foreign state actors; and what Canada is doing regarding this threat. Provides top tips for critical infrastructure owners and operators.

Barrett, M. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework*. NIST.

https://doi.org/10.6028/NIST.CSWP.04162018

The NIST Cybersecurity Framework provides a risk management framework for managing cybersecurity-related risks for critical infrastructure systems.

References

[1] Canadian Centre for Cyber Security. (2018, December 7). *Increasing Cyber Threat Exposure.* Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/increasing-cyber-threat-exposure

[2] Fortinet. (n.d.). *What is Operational Technology (OT): An Operational Technology Security Primer.* Fortinet. Retrieved January 26, 2022, from: https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security

[3] Public Safety Canada. (2009). *National Strategy for Critical Infrastructure.* Public Safety Canada. 2. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

[4] Public Safety Canada. (2009). *National Strategy for Critical Infrastructure.* Public Safety Canada. 4. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

[5] OECD. (2019). Good Governance for Critical Infrastructure Resilience (OECD Reviews of Risk Management Policies). OECD Publishing. https://doi.org/10.1787/02f0e5a0-en

[6] Fortinet. (2010). *Securing SCADA Infrastructure.* Fortinet. https://www.techdata.ca/techsolutions/networking/whitepapers/dec2010/Fortinet_Securing_SCADA_Infrastructure.pdf

[7] Office of the Fire Marshal & Emergency Management. *Hazard Identification Report 2019. Section F: Public Safety and Security Hazards.* Office of the Fire Marshal. https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/HIRA/Report/SectionF.html

[8] Ibid.

[9] Hildick-Smith, A. (2005). *Security for Critical Infrastructure SCADA Systems.* SANS Institute. https://www.sans.org/white-papers/1644/

[10] Miller, B., & Rowe, D. (2012, October). A survey SCADA of critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology (RIIT '12)*. Association for Computing Machinery, New York, NY, USA, 51–56. DOI: https://doi-org.ezproxy.lib.ryerson.ca/10.1145/2380790.2380805

[11] Public Safety Canada. (2021). *National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx

[12] Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies. (n.d.). *Cybersecurity and Infrastructure Security Agency*. Retrieved January 16, 2022, from https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

[13] Zetter, K. (2015, March 23). Stealing Data From Computers Using Heat. *Wired*. https://www.wired.com/2015/03/stealing-data-computers-using-heat/

[14] Fortinet. (2021). *Securing Industrial Control Systems with Fortinet: IEC-62443 Compliance End-to-End Security*. Fortinet. 3. https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Securing-Industrial-Control-Systems-with-Fortinet.pdf

[15] Chhillar, S. (n.d.). Common ICS Cybersecurity Myth #1: The Air Gap. International Society of Automation. Retrieved January 16, 2022, from https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap

[16] Ahmed, O. (2021, October 22). [Personal communication].

[17] Canadian Centre for Cyber Security. (2021, December 9). *Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021

[18] Johansen, A. (2021, November 23). *What is ransomware and how to help prevent ransomware attacks.* Norton. https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

[19] Check Point. (n.d.). *What is Ransomware?* Check Point Software Technologies LTD. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

[20] Tunney, C. (2021a, December 6). *Canadian energy, health, manufacturing sectors were major targets of ransomware attacks: cyber spy agency*. CBC News. https://www.cbc.ca/news/politics/ransomware-critical-infrastructure-cse-1.6274982

[21] Association of Municipalities Ontario. (2020). *A Municipal Cyber Security Toolkit: Best Practices to Guide and Improve Cyber Security Readiness*. Association of Municipalities Ontario. https://www.amo.on.ca/sites/default/files/assets/DOCUMENTS/Reports/2020/AMunicipalCyberSecurityToolkit20200930.pdf

[22] City of Stratford. (2019). *Ransomware Attack—Questions and Answers*. City of Stratford. https://www.stratford.ca/en/inside-city-hall/resources/ReportsAndPublications/cyber_incident_q_and_a.pdf

[23] Valiante, G. (2018, November 18). *'Quebec is an embarrassment': Province urged to do more on cybersecurity.* CBC News. https://www.cbc.ca/news/canada/montreal/quebec-cyberattacks-local-governments-1.4910720

[24] Turton, W., & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg.* https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[25] Ibid.

[26] Sanger, D. E., & Perlroth, N. (2021, May 14). Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity. *The New York Times.* https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

[27] Tunney, C. (2021a, December 6). *Canadian energy, health, manufacturing sectors were major targets of ransomware attacks: cyber spy agency.* CBC News. https://www.cbc.ca/news/politics/ransomware-critical-infrastructure-cse-1.6274982

[28] CBC News. (2021, December 6). Over a month after the cyberattack on health care in N.L. began, Furey is still mum on details. *CBC.ca.* https://www.cbc.ca/news/canada/newfoundland-labrador/cyber-attack-furey-1.6275764

[29] Roberts, D. (2021, December 14). Some patient SINs stolen in N.L. cyberattack. *CBC.ca.* https://www.cbc.ca/news/canada/newfoundland-labrador/cyberattack-update-dec-14-1.6285285

[30] CBC News. (2021, December 6). Over a month after the cyberattack on health care in N.L. began, Furey is still mum on details. *CBC.ca.* https://www.cbc.ca/news/canada/newfoundland-labrador/cyber-attack-furey-1.6275764

[31] Solomon, H. (2021a, October 30). Toronto Transit Commission still recovering from ransomware attack. *IT World Canada.* https://www.itworldcanada.com/article/toronto-transit-commission-still-recovering-from-ransomware-attack/463683

[32] Canadian Manufacturers and Exporters. (2012), *Manufacturing Our Future: A Manufacturing Action Plan for Canada Driving Investment, Creating Jobs, Growing Exports, Canadian Manufacturers and Exporters*. Canadian Manufacturers and Exporters.

[33] Natural Resources Canada. (2021, August 6). *Protecting Canada's Energy Supply Chains From Cyber Threats* [News releases]. Government of Canada. https://www.canada.ca/en/natural-resources-canada/news/2021/08/protecting-canadas-energy-supply-chains-from-cyber-threats.html

[34] European Union Agency for Cybersecurity. (2021). *ENISA Threat Landscape for Supply Chain Attacks*. European Union Agency for Cybersecurity. https://doi.org/10.2824/168593

[35] North American Electric Reliability Corporation. (2021). *2021 State of Reliability: An Assessment of 2020 Bulk Power System Performance*. North American Electric Reliability Corporation. 73. https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2021.pdf

[36] Newman, L. H. (2020, December 19). How to Understand the Russia Hack Fallout. *Wired*. https://www.wired.com/story/russia-solarwinds-hack-targets-fallout/; CISA. (2021, April 15). *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*. CISA. https://www.cisa.gov/uscert/ncas/alerts/aa20-352a

[37] Newman, L. H. (2020, December 19). How to Understand the Russia Hack Fallout. *Wired*. https://www.wired.com/story/russia-solarwinds-hack-targets-fallout/

[38] Fruhlinger, J. (2020, September 4). *What is phishing? How this cyber attack works and how to prevent it*. CSO. https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

[39] Ibid.

[40] U.S. Department of the Treasury. (2020, October 23). *Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/sm1162

[41] City of Burlington. (2019, June 13). *City of Burlington reports online fraud*. City of Burlington. https://www.burlington.ca/en/Modules/News/index.aspx?newsId=7154f07d-58dc-4bdb-b723-d59372f4f9c2

[42] FireEye. (n.d.). *What is a Zero-Day Exploit?* FireEye. Retrieved January 21, 2022, from https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

[43] CBC News. (2019, January, 21). *Containing the virus: what made HSN computer attacker such a nuisance? CBC.ca*. https://www.cbc.ca/news/canada/sudbury/zero-day-hsn-1.4986611

[44] Weisman, S. (2020, July 23). *What is a distributed denial of service attack (DDoS) and what can you do about them?* Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

[45] Ibid.

[46] Tremblay, B. (2014, July 31). *Chinese cyberattack targets Orangeville municipal network*. Orangeville.com. https://www.orangeville.com/news-story/4730336-chinese-cyberattack-targets-orangeville-municipal-network/

[47] Ibid.

[48] Daily Herald. (2021, August 19). SUMA calls on federal parties to make commitments in Federal Election. *Prince Albert Daily Herald*. https://paherald.sk.ca/2021/08/19/suma-calls-on-federal-parties-to-make-commitments-in-federal-election/

[49] Swanson, D., Murphy, D., Temmer, J., & Scaletta, T. (2021). *Advancing the Climate Resilience of Canadian Infrastructure*. International Institute for Sustainable Development. https://www.iisd.org/system/files/2021-07/climate-resilience-canadian-infrastructure-en.pdf

[50] Tunney, C. (2021, August 27). *Municipalities ask Ottawa for billions of dollars to protect themselves from climate change*. CBC News. https://www.cbc.ca/news/politics/fcm-climate-election-1.6154370

[51] Canadian Centre for Cyber Security. (2018, December 7). *Increasing Cyber Threat Exposure*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/increasing-cyber-threat-exposure

[52] Bailey, T., Maruyama, A., & Wallance, D. (2020). The energy sector threat: How to address cybersecurity vulnerabilities. *McKinsey and Company*. https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

[53] Henderson, J. (2021, September 20). *Bridging the Municipal Funding Gap series: Problems on the horizon. St. Albert Today*. https://www.stalberttoday.ca/local-news/bridging-the-municipal-funding-gap-series-problems-on-the-horizon-4329687

[54] Bristow, M. (2021). *A SANS 2021 Survey: OT/ICS Cybersecurity*. SANS Institute. https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

[55] Fortinet. (2020). *Fortinet Survey Finds Widespread Impact from Cybersecurity Skills Shortage*. Fortinet. https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-fortinet-survey-skills-shortage.pdf

[56] Fernandes, M. (2022, January 25). [Personal communication].

[57] White, C., Palmer, L., & Williams, D. (2021, November 5). [Personal communication].

[58] Schultz, D. (2021, November 25). [Personal communication].

[59] Spicer, Z. (2021, November 9). [Personal communication].

[60] Public Safety Canada. (2019, January 21). *Fundamentals of Cyber Security for Canada's CI Community*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx

[61] Czerny, A. (2022, February 22). [Personal communication].

[62] Service Alberta. (2021). *Cybersecurity Strategy: Protecting the Province's Information and Technology Assets*. Government of Alberta. 15. https://open.alberta.ca/dataset/1d988471-642e-4de3-a046-ca05449e7a08/resource/c53eca57-042b-497d-a16e-3868d889885d/download/sa-goa-cybersecurity-strategy-protecting-provinces-digital-assets-annual-update-2021.pdf

[63] Ibid, 15.

[64] Ministers Responsible For Emergency Management. (2017). *An Emergency Management Framework for Canada—Third Edition*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-en.aspx

[65] Office of the Fire Marshal & Emergency Management. (2019). *Methodology Guidelines 2019*. Ontario Ministry of the Solicitor General. https://web.archive.org/web/20210708193732/https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/HIRA/Guidelines/main.html

[66] Office of the Fire Marshal & Emergency Management. (2019). *Hazard Identification Report 2019—Section F - Public Safety and Security Hazards | Emergency Management Ontario*. Ontario Ministry of the Solicitor General. https://web.archive.org/web/20210708192819/https://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/HIRA/Report/SectionF.html#Cyber

[67] North American Electric Reliability Corporation. (n.d.). *North America*. North American Electric Reliability Corporation. Retrieved January 24, 2022, from https://www.nerc.com/AboutNERC/keyplayers/Pages/Canada.aspx

[68] NERC. (2022). *Canadian Provincial Summaries of Standard-Making and Enforcement Functions with U.S. Comparators*. NERC. https://web.archive.org/web/20220308173542/https://www.nerc.com/AboutNERC/keyplayers/Documents/Canadian-Provincial-Summaries.pdf

[69] Natural Resources Canada. (2016, July 20). *Newfoundland and Labrador's Electric Reliability Framework*. Natural Resources Canada; Natural Resources Canada. https://www.nrcan.gc.ca/energy/electricity-infrastructure/electricity-canada/canada-electric-reliability-framework/newfoundland-and-labradors-electric-reliability-framework/18834;

[70] Environment and Sustainable Resource Development. (2012). Part 2: Guidelines for municipal waterworks. In *Standards and guidelines for municipal waterworks, wastewater and storm drainage systems*. Alberta Queen's Printer. 51. https://open.alberta.ca/dataset/5668185/resource/eb117384-bf6a-4db5-9290-5971ecb42a9f

[71] Ibid, 51.

[72] Government of Ontario. (2019, May 27). *Design Guidelines for Drinking-Water Systems: Instrumentation & control and distribution systems*. Government of Ontario. https://www.ontario.ca/document/design-guidelines-drinking-water-systems/instrumentation-control-and-distribution-systems

[73] Hollister, A. (2021, June 28). *Cybersecurity and the water supply: managing a growing risk worldwide. LogRhythm*. https://logrhythm.com/blog/cybersecurity-and-the-water-supply-managing-a-growing-risk-worldwide/

[74] Government of New Brunswick. (2018). *Digital New Brunswick Strategy Document*. Government of New Brunswick. https://www2.gnb.ca/content/dam/gnb/Departments/eco-bce/Promo/digitalnb/digital_new_brunswick.pdf

[75] Green, W. (2021, May 17). Just 5% of firms assess cyber risk in wider supply chain. *CIPS*. https://www.cips.org/supply-management/news/2021/may/just-5-of-firms-assess-cyber-risk-in-wider-supply-chain/

[76] BOMA Canada. (2020). *2020 Cyber Wellness Guide: Embedding Cybersecurity in Procurement*. BOMA Canada. https://bomacanada.ca/wp-content/uploads/2019/11/BOMA_Cyber_Procurement_Guide.pdf

[77] Ibid.

[78] Government of Ontario. (2021, October 1). *Municipal asset management planning*. Government of Ontario. http://www.ontario.ca/page/municipal-asset-management-planning

[79] Ordr. (2021, July 2). *The Increasing Importance of Cybersecurity Asset Management*. Ordr. https://ordr.net/article/increasing-importance-of-cybersecurity-asset-management

[80] Hydro-Québec. (n.d.). *Reliability standards and functional entities*. Hydro-Québec. Retrieved January 24, 2022, from https://www.hydroquebec.com/reliability-coordinator/reliability-news/reliability-news-standards-funtional-entities.html

[81] Marron, J., Gopstein, A., & Bogle, D. (2021). *Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.09292021

[82] Ibid.

[83] *Who we are*. (n.d.). Ontario Energy Board. Retrieved January 26, 2022, from https://www.oeb.ca/about-oeb/who-we-are

[84] Ontario Energy Board. (2017). *Ontario Cyber Security Framework*. Ontario Energy Board. https://www.oeb.ca/sites/default/files/Ontario-Cyber-Security-Framework-20171206.pdf

[85] *The Ontario Gazette: Government Notices—Other | Ontario.ca*. (2018, April 6). Government of Ontario. https://www.ontario.ca/document/ontario-gazette-volume-151-issue-14-april-7-2018/government-notices-other; Freedman, B., & Vellone, J. A. D. (2018, March 23). *Cybersecurity Framework for Ontario's Electricity Industry*. Borden Ladner Gervais LLP. https://www.blg.com/en/insights/2018/03/cybersecurity-framework

[86] Solomon, H. (2019, January 18). Ontario electric utilities to report soon on their cyber security maturity | IT World Canada News. *IT World Canada*. https://www.itworldcanada.com/article/ontario-electric-utilities-to-report-soon-on-their-on-cyber-security-maturity/414233

[87] Anonymous participant. (2021, November 25). [Personal communication].

[88] Ibid.

[89] Fernandes, M. (2022, January 25). [Personal communication].

[90] OECD. (2019). Good Governance for Critical Infrastructure Resilience (OECD Reviews of Risk Management Policies). OECD Publishing. https://doi.org/10.1787/02f0e5a0-en

[91] U.S. Department of State & Cybersecurity and Infrastructure Security Agency. (2019). *A Guide to Critical Infrastructure Security and Resilience*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience

[92] North American Electric Reliability Corporation. (n.d.). *Electricity Information Sharing and Analysis Center*. North American Electric Reliability Corporation. Retrieved January 24, 2022, from https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx

[93] Miller, M. (2021, November 18). Hundreds participate in electric grid cyberattack simulation amid increasing threats. *The Hill*. https://thehill.com/policy/cybersecurity/582246-hundreds-participate-in-electric-grid-cyberattack-simulation-amid

[94] Public Safety Canada. (2020, November 24). The Canadian Cyber Security Tool (CCST). Public Safety Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-scrt-tl/index-en.aspx

[95] Ibid.

[96] Schultz, D. (2021, November 25). [Personal communication].

[97] Public Safety Canada. (2018, December 21). Cyber & Infrastructure Resilience Assessments. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx

[98] Infrastructure Canada. (2021). *Building Pathways to 2050: Moving Forward on the National Infrastructure Assessment*. Government of Canada. https://www.infrastructure.gc.ca/alt-format/pdf/nia-eni/nia-eni-2-en1.pdf

[99] Czerny, A. (2022, February 22). [Personal communication].

[100] Participant name withheld. . (2022, January). [Personal communication].

[101] Sorrey, R. (2021, November 9). [Personal communication].

[102] Schultz, D. (2021, November 25). [Personal communication].

[103] *MISA ON Industry Insight: How City of Lethbridge strengthened their security posture*. (n.d.). MISA/ASIM. Retrieved January 26, 2022, from https://www.misa-asim.ca/events/EventDetails.aspx?id=1525018

[104] Association of Municipalities Ontario. (2020). *A Municipal Cyber Security Toolkit: Best Practices to Guide and Improve Cyber Security Readiness*. Association of Municipalities Ontario. https://www.amo.on.ca/sites/default/files/assets/DOCUMENTS/Reports/2020/AMunicipalCyberSecurityToolkit20200930.pdf

[105] Schultz, D. (2021, November 25). [Personal communication].

[106] Association of Municipalities Ontario. (2020). *A Municipal Cyber Security Toolkit: Best Practices to Guide and Improve Cyber Security Readiness*. Association of Municipalities Ontario. https://www.amo.on.ca/sites/default/files/assets/DOCUMENTS/Reports/2020/AMunicipalCyberSecurityToolkit20200930.pdf

[107] Oldman, C. (2021, October 28). [Personal communication].

[108] Ahmed, O. (2021, October 22). [Personal communication].

[109] Hope, A. (2022, February 22). One in Seven Ransomware Attacks on Critical Infrastructure and Industrial Systems Expose Sensitive OT Information. *CPO Magazine*. https://www.cpomagazine.com/cyber-security/one-in-seven-ransomware-attacks-on-critical-infrastructure-and-industrial-systems-expose-sensitive-ot-information/

[110] Spicer, Z. (2021, November 9). [Personal communication].

[111] Association of Municipalities Ontario. (2020). *A Municipal*

Cyber Security Toolkit: Best Practices to Guide and Improve Cyber Security Readiness. Association of Municipalities Ontario. https://www.amo.on.ca/sites/default/files/assets/DOCUMENTS/Reports/2020/AMunicipalCyberSecurityToolkit20200930.pdf

[112] Czerny, A. (2022, February 22). [Personal communication].

[113] Sorrey, R. (2021, November 9). [Personal communication]; Schultz, D. (2021, November 25). [Personal communication].

[114] European Union Agency for Cybersecurity. (2021). *ENISA Threat Landscape for Supply Chain Attacks*. European Union Agency for Cybersecurity. 27. https://doi.org/10.2824/168593

[115] Bristow, M. (2021). *A SANS 2021 Survey: OT/ICS Cybersecurity*. SANS Institute. https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/

[116] Miller, G. (2021, June 22). Prepare For the Worst, Hope For the Best. *ReNew Canada*. https://www.renewcanada.net/feature/prepare-for-the-worst-hope-for-the-best

[117] National Institute of Standards and Technology. (n.d.). *Best Practices in Cyber Supply Chain Risk Management*. National Institute of Standards and Technology. Retrieved January 17, 2022, from https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[118] Ibid.

[119] Zaslavsky, I. (2022, February 9). [Personal communication].

[120] Federation of Canadian Municipalities & Insurance Bureau of Canada. (2020). *Investing in Canada's Future: The Cost of Climate Adaptation at the Local Level*. Federation of Canadian Municipalities and Insurance Bureau of Canada. https://data.fcm.ca/documents/reports/investing-in-canadas-future-the-cost-of-climate-adaptation.pdf

[121] Romeo-Beehler, B. (2020). *Cyber Safety—Critical Infrastructure Systems: Toronto Water SCADA System*. City of Toronto Auditor General's Office. https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-145342.pdf

[122] Deloitte & Toronto Financial Services Alliance. (2018). *The Changing Faces of Cybersecurity: Closing the Cyber Risk Gap*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

[123] Public Safety Canada. (2009). *National Strategy for Critical Infrastructure*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

[124] Canadian Electricity Association. (2021). U.S. Department of Energy Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure. Canadian Electricity Association. https://www.energy.gov/sites/default/files/2021-06/Grace%20Dickson%20Denton-A1.pdf

[125] North American Electric Reliability Corporation. (2021). *2021 State of Reliability: An Assessment of 2020 Bulk Power System Performance*. North American Electric Reliability Corporation. https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2021.pdf

[126] Round-tableRound table participant. (2022, February 18. [Personal communication].

[127] Association of Municipalities Ontario. (2020). *A Municipal Cyber Security Toolkit: Best Practices to Guide and Improve Cyber Security Readiness*. Association of Municipalities Ontario. https://www.amo.on.ca/sites/default/files/assets/DOCUMENTS/Reports/2020/AMunicipalCyberSecurityToolkit20200930.pdf

[128] Public Safety Canada. (2019, January 21). *Fundamentals of Cyber Security for Canada's CI Community*. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx

[129] Siu, K. (2021, November 23). [Personal communication].

[130] Participant name withheld. (2022, January). [Personal communication].