

The State of Cybersecurity in Canada 2025

PREPARED BY Canadian Cybersecurity Network
and Security Architecture Podcast



Contents

5

Introduction

6

Executive Summary

By François Guay, Evgeniy Kharam and Dmitry Raidman

8

Config Chaos | How IoT and Cloud misconfigurations undermine security
By Antoinette Hodes, Evangelist & Global Solution Architect, Presented by Check Point Software Technologies

12

Milestones that are important to Canada and cyber

By Bob Gordon

17

Facing the Cyber Storm: Canada's Path to Building Resilience in 2025

By J. Paul Haynes

21

Securing Digital Frontiers: Tackling Cybersecurity and Privacy Challenges in 2025

By Michael Argast

24

The State of AI in Canada

By Helen Oakley

29

Bridging the cybersecurity gaps: Preparing for change in 2025

Presented By Mastercard

32

Providing Cyber Security in Real Time

By Paul Da Silva

36

Strengthening Cybersecurity in Canada's Public Sector: Key Insights and Strategic Recommendations

By Deryck Greer

40

Cyber Risk Can't Be Solved With Technology Alone

By David Shipley

47

Securing excellence: A guide to an information security management system

By Caio Cologni

Presented by BSI Canada

50

The Cyber Insurance Market

By Jonathan Weekes

54

A Novel Approach to Data Protection

By Christopher Lee

Presented by GlassHouse Systems

58

Building Resilience Through Cybersecurity Awareness

By Junior Williams

62

Securing Digital Identity in an AI-Driven World

By Fahad Kabir, Presented by

IAMConcepts Security Solutions Inc.

65

The Canadian Threat Landscape

By Julien Richard

70

The State of Third-Party Cyber Risk Management in Canada

Presented by BlueVoyant

72

Cybersecurity for Canadian Digital Infrastructure

By Albert Heine

75

The State of Software Supply Chain Security in Canada

By Dmitry Raidman

78

State of Cybersecurity in Canadian Retail

By Isaac Wanzama

84

Safeguarding Canada's Power: Cybersecurity Landscape in Energy & Utilities

By Denrich Sanada and

Sonia Khan

88

Beyond the Badge: Cybercrime Challenges and Solutions in Modern Policing

By Lina Dabit

91

Canada's Education Sector: A Low-Hanging Fruit for Cyber Criminals?

By Lester Chng

94

Addressing the talent gap: Focusing on mid-career transitions

By Randy Purse

99

Buggy Code: An In-Depth Look at the Cybersecurity Job Market

By François Guay

102

Key Recommendations

Contributors



Bob Gordon



J. Paul Haynes



Michael Argast



Helen Oakley



Paul Da Silva



Deryck Greer



David Shipley



Jonathan Weekes



Junior Williams



Fahad Kabir



Julien Richard



Albert Heine



Dmitry Raidman



Isaac Wanzama



Denrich Sanada



Lina Dabit



Lester Chng



Randy Purse



François Guay

Features



Config Chaos | How IoT and Cloud misconfigurations undermine security
By Antoinette, Hodes, Evangelist & Global Solution Architect,
Presented by Check Point Software Technologies

29

Bridging the cybersecurity gaps:
Preparing for change in 2025
Presented by Mastercard

47

Securing excellence: A guide
to an information security
management system
By Caio Cogni
Presented by BSI Group

54

A Novel Approach to Data Protection
By Christopher Lee
Presented by GlassHouse Systems

62

Securing Digital Identity in
an AI-Driven World
By Fahad Kabir
Presented by IAMConcepts Security
Solutions Inc.

70

The State of Third-Party Cyber Risk
Management in Canada
Presented by BlueVoyant

*Thank you to our sponsors listed in
order of appearance.*

Introduction

by [François Guay](#), [Evgeniy Kharam](#)
and [Dmitry Raidman](#)

Over the past year, Canadian organizations and institutions have witnessed a dramatic surge in cyber incidents, from ransomware attacks crippling critical infrastructure to the exploitation of vulnerabilities in cloud systems, IoT devices, and supply chain security. These attacks have inflicted financial damage, disrupted essential services, and eroded public trust. In a landscape where state-sponsored actors, cybercriminals, and opportunistic threat actors operate with increasing efficiency, the urgency to develop robust cybersecurity strategies has never been greater.

As you navigate through the 2025 State of Cybersecurity Report, our hope is that it will serve as both an informative resource and a call to action.

The State of Cybersecurity Report in Canada 2025, serves as both an informative resource and a rallying cry for Canadian leaders. It challenges them to address cybersecurity not just as a challenge but as a driver of growth and innovation. It is also a celebration of Canadian thought leadership on very important business and technology topics that are directly impacting Canadians quality of life as well as their pocketbooks.

Supply chain security and asset risk-based management have emerged as critical focal points as organizations face growing threats stemming from third-party vulnerabilities and increasingly complex digital ecosystems. The security of supply chains—particularly in software dependencies and asset management—presents cascading risks that require advanced tools and strategies to address.

Emerging technologies like Agentic AI and advances in Identity Threat Detection and Response (ITDR) are reshaping the cybersecurity landscape. While these innovations offer tools to enhance defense capabilities, they also present new vulnerabilities, such as enabling sophisticated phishing campaigns, deepfake attacks, and the exploitation of digital identities. IoT and cloud misconfigurations have further amplified the attack surface, leaving critical industries such as healthcare, energy, retail, and education vulnerable to disruptions.

Compounding these challenges is a persistent cybersecurity talent gap, with 10,000 to 25,000 unfilled positions expected in the near term. This shortage affects the ability of organizations to adapt to the evolving threat landscape and undermines national resilience. Addressing this gap requires collaborative efforts to reskill professionals and make cybersecurity education more accessible across regions.

As you navigate through the 2025 State of Cybersecurity Report, our hope is that it will serve as both an informative resource and a call to action. Whether you are a business leader, policymaker, educator, or cybersecurity practitioner, this report is designed to equip you with the knowledge and insights needed to navigate today's challenges and build resilience for the future. Together, we can safeguard Canada's digital frontiers and turn cybersecurity from a reactive necessity into a strategic enabler of progress and innovation. [@](#)

Executive Summary

In the winter of 2024, a sophisticated ransomware attack brought one of Canada's largest healthcare networks to a grinding halt. Patient care was disrupted, surgeries postponed, and sensitive data threatened. This breach, like many others in recent years, underscored the growing vulnerability of critical sectors across Canada. As organizations race to adopt advanced technologies, cybercriminals exploit gaps in security, leaving the nation's economy and public trust at risk. These events serve as a stark reminder that Canada's cybersecurity must evolve swiftly to keep pace with the escalating threat landscape.

The 2025 State of Cybersecurity Report delivers an in-depth analysis of the evolving cyber landscape in Canada, drawing on insights from various sectors and expert analyses. This report highlights urgent cybersecurity challenges while presenting actionable strategies for strengthening Canada's digital resilience.

Key Findings

RISING THREATS:

Canadian sectors, especially healthcare, energy, education, and retail, have become prime targets for cybercriminals. Breaches are increasingly linked to human error and systemic vulnerabilities, with IoT and cloud misconfigurations accounting for 82% of breaches. As Paul Da Silva notes,

"Ransomware is no longer a question of if but when. Canadian businesses must adopt a proactive, layered defense strategy to mitigate this inevitability."

TALENT SHORTAGE:

Canada's cybersecurity workforce faces a significant deficit, producing fewer than 4,000 graduates annually compared to the demand for up to 25,000 roles. This gap threatens economic stability and public safety. Randy Purse emphasizes,

"The cybersecurity skills gap is a national risk, threatening our economy and public safety. Mid-career transitions and regional training initiatives are essential for addressing this challenge."

EMERGING TECHNOLOGIES:

Generative AI, while aiding defensive measures, also enables sophisticated attacks like deepfake-based fraud and identity theft. ITDR (Identity Threat Detection and Response) has emerged as a critical strategy to combat these threats, addressing identity vulnerabilities in cloud and hybrid environments.

Sector-Specific Challenges

- **Energy:** Legacy OT systems and supply chain dependencies make the sector vulnerable to ransomware and insider threats, with 75% of energy companies identifying supply chain risks as a top concern.
- **Education:** Insufficient funding and governance issues leave institutions exposed to ransomware and data breaches, disrupting academic operations.
- **Retail:** Third-party vulnerabilities and data breaches cost the sector \$7.05 million per breach on average, with digital transformation heightening risks.

Collaboration and Policy Innovation

Cross-sector collaboration is pivotal for cybersecurity resilience. Organizations must also focus on fostering a security culture and adopting standards like ISO/IEC 27001, which strengthen resilience through structured governance and proactive measures.

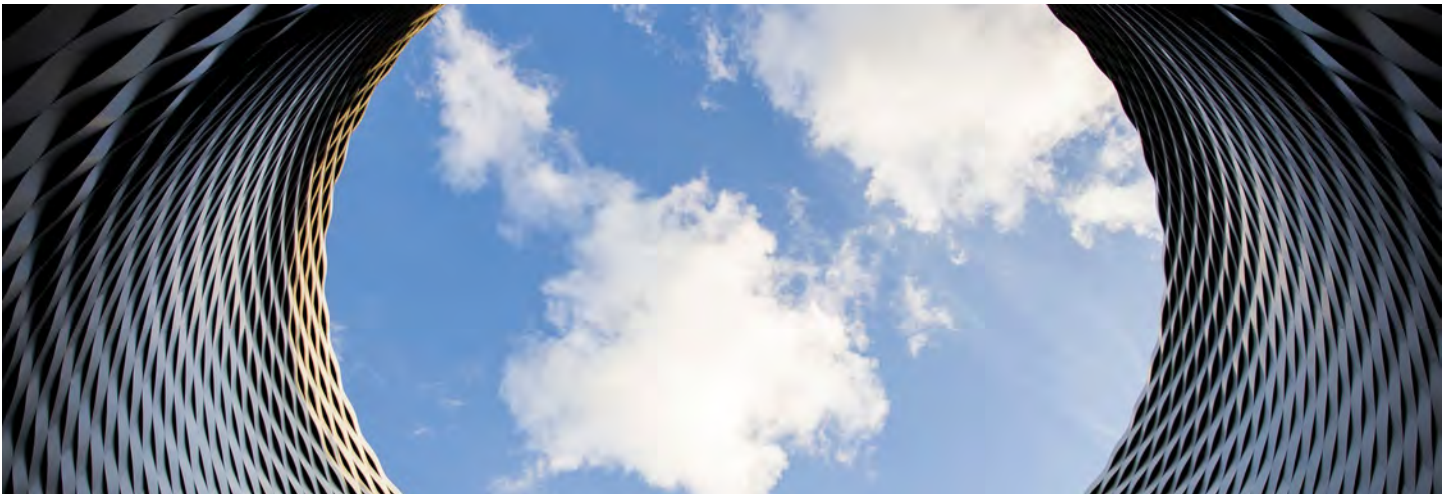
As Canada faces escalating cyber risks, this report underscores the importance of a national strategy integrating advanced technologies, policy innovation, and workforce development. With bold action and united efforts, Canada can secure its digital future against growing threats. @

CHECK POINT DRIVES THE WAY AS THE LEADING CYBER SECURITY PLATFORM

AI-Powered. Cloud-Delivered.
That's Security in **Action.**

checkpoint.com/action





Config Chaos | How IoT and Cloud misconfigurations undermine security

by [Antoinette Hodes](#), Evangelist & Global Solution Architect, Presented by Check Point Software Technologies

In an increasingly connected world, IoT and cloud infrastructures are the backbone of modern innovation. As IoT evolves, it intertwines with hybrid APIs—essential for communication between IoT devices and the cloud—serve as both lifelines and attack vectors.

Yet, as these technologies integrate deeper into our lives and businesses, they introduce hidden vulnerabilities—misconfigurations—that few fully understand. These oversights are no longer merely technical glitches; they are amplifiers of systemic risk, creating cascading failures across the digital ecosystem and staggering costs. Human error is also a common cause for misconfiguration. According to [Verizon's Data Breach investigation report](#), human error is responsible for 82% of data breaches. Let's explore how these vulnerabilities emerge and challenges emerging in IoT-cloud ecosystems.

How simple mistakes lead to complex breaches

IOT | A GROWING ATTACK SURFACE

IoT devices are often rushed to market with minimal security considerations. This trend is driven by several factors, including the intense competition to be the first to offer a particular feature in the market, as well as budget constraints that often limit the resources allocated to thorough security testing and design. Default credentials, open ports and inadequate or even no update mechanisms are the most common issues. However, deeper misconfigurations

like unsecured MQTT (Message Queuing Telemetry Transport) brokers can lead to unauthorized access and massive data leaks. Think of MQTT brokers like post offices that handle messages. The problem lies not only in the devices but also in how they interact with networks, and each other. Their widespread adoption means billions of devices are connected globally, ranging from smart home assistants to industrial control systems. Here's why IoT security is particularly precarious:

- **Default credentials:** Many IoT devices are shipped with default usernames and passwords, which users often fail to change, making them easy targets for attackers.
- **Lack of updates:** Manufacturers frequently deprioritize firmware updates, leaving vulnerabilities unpatched.
- **Limited visibility:** IoT devices often operate in shadow IT environments, escaping the notice of security teams.

When IoT devices are integrated into cloud systems, these vulnerabilities don't just remain localized, they are amplified.

CLOUD MISCONFIGURATIONS | A CATALYST FOR EXPLOITATION

Cloud services promise scalability and convenience but demand precision in setup. A simple misstep, such as leaving a storage bucket public or mismanaging Identity and Access Management (IAM) roles, can expose critical assets to the internet. Worse still, the nature of cloud environments

means that vulnerabilities can propagate across regions and accounts, amplifying their impact. A [report from XM Cyber](#) which analysed 40 million exposures, states that 80% of exposures are caused by identity and credential misconfigurations. Then we have improperly configured databases. Common missteps include:

- Publicly accessible storage buckets: Sensitive data stored in cloud buckets often lacks proper access controls, leading to breaches.
- Weak identity and access management (IAM): Misconfigured permissions can allow attackers to escalate privileges and access critical resources.
- Overlooked default settings: Cloud services often come with default settings that prioritize usability over security.

These misconfigurations act as a gateway for attackers, who exploit IoT weaknesses to gain a foothold in the cloud.

80%

of security breaches are caused by identity and credential misconfiguration.

The anatomy of misconfigurations

The role of APIs in IoT and cloud ecosystems cannot be overstated. APIs are the backbone of IoT and cloud integration, facilitating everything from device management to data transfer in real time. However, they are also one of the most exploited components in these environments. Misconfigured or poorly secured APIs can:

- Expose sensitive device telemetry to unauthorized users.
- Allow attackers to manipulate data streams or device functionality.
- Serve as entry points for lateral movement within hybrid cloud infrastructures.

For instance, API keys embedded in IoT firmware can be extracted and reused by attackers to compromise entire cloud-hosted IoT fleets.

Open ports, open doors | How much of IoT security is misconfiguration-driven?

[Microminder's report](#) is stating that 80% of security breaches are caused by identity and credential misconfiguration. This figure dwarfs other common IoT vulnerabilities such as unpatched software or outdated firmware. While the percentage varies depending on the industry and use case, misconfiguration is a dominant factor across smart homes, industrial IoT (IIoT), and healthcare devices.

Why misconfigurations amplify threats

1. ATTACK SURFACE MULTIPLICATION

The quiet growth of IoT and cloud vulnerabilities IoT ecosystems and cloud environments are vast, dynamic and interconnected. A misconfigured IoT camera, for instance, can serve as an entry point to an entire corporate network. A misconfigured cloud service, video stream can expose sensitive customer data.

2. BLIND SPOTS IN DETECTION

How blind spots erode your security posture Misconfigurations often fly under the radar of traditional security monitoring tools. Attackers exploit these blind spots, leveraging tools like Shodan to scan for vulnerable IoT devices or misconfigured cloud assets.

3. SPEED OF EXPLOITATION

Why IoT devices can't afford delayed security Once discovered, misconfigurations can be exploited within minutes. Attackers use automated tools to weaponize these errors at scale, launching botnets or ransomware campaigns.

When IoT and Cloud turn into Toxic Combinations

IoT and the cloud can be a dangerous cocktail of risk when misconfigurations meet overprivileged access and insecure design. Picture a cloud-based virtual machine with exploitable vulnerabilities, exposed to the internet, with overprivileged access deeper into the cloud account or on-premises networks. This is granting attackers a bridge to the cloud or your network. Now, amplify that threat through IoT devices, like cheap cameras or sensors - offering cloud connectivity by default. These devices can become invisible conduits of risk, syncing to poorly configured cloud storage that leaks

data or even pulling firmware updates from a compromised source. A single exploited IoT device connected to the cloud can transform into an entry point for attackers, propagating botnets, data breaches and supply chain havoc. As more OEM providers bake insecure cloud dependencies into their IoT products, the potential for unseen exploitation scales dramatically, endangering businesses and consumers alike.

15%

of consumers never change default settings.

What no one talks about

1. DEFAULT CONFIGURATIONS ARE EVERYWHERE

Many IoT devices hold default usernames and passwords. These credentials are often available online, making them a goldmine for attackers. Shockingly, 15% of consumers never change default settings, exposing their devices to automated botnet scans.

2. SHADOW IOT IS GROWING UNCHECKED

Shadow IoT devices, unauthorized or unknown devices on a network worsen the misconfiguration problem.

3. PROTOCOL PITFALLS

Protocols like MQTT and CoAP, widely used in IoT, are often deployed without proper security measures.

4. MISCONFIGURATIONS IN THE CLOUD BACKEND

IoT devices often rely on cloud-based platforms. Misconfigured cloud storage buckets or APIs linked to IoT devices account are often ignored in traditional IoT security discussions.

Why hybrid clouds complicate security

Hybrid cloud environments, combining public and private clouds, provide IoT ecosystems with scalability and resilience. However, their complexity introduces unique challenges:

- **Misaligned security policies:** Different security configurations across private and public clouds can create gaps. For example, an IoT device connecting to a private cloud might adhere to stringent encryption protocols, while its connection to a public cloud uses weaker settings.
- **Data residency and transfer risks:** Telemetry data often moves across borders in hybrid setups, potentially violating compliance rules if misconfigured.
- **Visibility challenges:** Traditional monitoring tools struggle to provide end-to-end visibility across hybrid clouds, making it harder to detect misconfigurations or breaches.

Other amplifications are data silos. Poorly configured APIs and access controls can isolate critical telemetry, leading to blind spots in monitoring. Attackers exploit these silos to remain undetected. Secondly, latency issues caused by misconfigured cloud regions can lead to delayed responses in IoT systems, impacting operations like predictive maintenance or real-time alerts. Lastly, misconfigurations in resource overlap can ripple through, affecting storage, compute, and network services simultaneously, as APIs often interact with multiple cloud resources.

Behind the buzzwords

IoT and cloud misconfigurations create a cascade of challenges that extend far beyond initial breaches. For IoT systems, the consequences often include physical damages such as equipment failures, safety risks or operational disruptions, all of which compound financial losses. In cloud environments, the aftermath can involve regulatory fines, customer lawsuits, and reputational damage that far exceed the initial response costs. These issues are further amplified by stringent compliance requirements under frameworks like the GDPR and the EU's Cyber Resilience Act (CRA), which impose heavy penalties for violations, especially on IoT products now under increased scrutiny. Worse still, misconfigurations rarely exist in isolation. In today's interconnected ecosystems, a single misconfigured IoT device, such as a CCTV camera can trigger a chain reaction, providing attackers with lateral access to critical infrastructure and amplifying the overall impact. This convergence

of compounding costs, regulatory risks, and chain reactions underscores the urgent need for meticulous configuration and proactive security management.

Key takeaways

1. MISCONFIGURATIONS ARE THE ACHILLES' HEEL OF IOT SECURITY

They are responsible for a significant portion of breaches yet are often overlooked in favour of more complex vulnerabilities.

2. DEFAULT CREDENTIALS AND OPEN PORTS ARE LOW-HANGING FRUIT FOR ATTACKERS

Basic hygiene like changing default passwords and closing unnecessary ports can mitigate many risks.

3. VISIBILITY IS KEY

Shadow IoT devices and poorly documented systems create blind spots in networks, increasing misconfiguration risks.

4. AUTOMATION TOOLS CAN HELP

Leveraging AI-powered tools to scan for misconfigurations can drastically reduce human error and enhance overall security.


5. HOLISTIC SECURITY APPROACHES ARE ESSENTIAL

It's not just about securing the device but also the network, cloud backend, and protocols it interacts with.

What Can We Do About It?

- **Educate users and organizations:** Many IoT vulnerabilities are avoidable with basic awareness and training.
- **Adopt strong device management:** Organizations must maintain visibility into connected devices and regularly audit configurations.
- **Advocate for secure defaults:** Manufacturers should ship devices with security-first configurations, minimizing user effort.
- **Regulate and enforce standards:** Policies like the EU Cyber Resilience Act (CRA) can incentivize better practices in device manufacturing and deployment.

Misconfigurations in IoT are often ignored until it's too late. By understanding the scale of the issue and taking proactive steps, we can prevent the next wave of attacks and secure the interconnected future we envision.

What do you think? Are organizations ready to face this misconfiguration pandemic? 



Milestones that are important to Canada and cyber

by [Bob Gordon](#)

Canada's cyber environment has undergone significant changes over the past twenty years resulting in noteworthy milestones. This article briefly describes those changes and the resulting milestones.

Advances in technology, and its broad adoption by governments, businesses, and individuals, have resulted in significant societal benefits. Unfortunately, criminals and some nation states, for example The People's Republic of China, Russia, and Iran, are using these advances for purposes that harm Canadians.¹ These activities were part of the impetus in establishing the milestones outlined below. Changes to the cyber environment are continuing and these will create new, un-identified, milestones.

The initial environmental change occurred around the turn of the century with Canadians' growing interest in the privacy of their personal information. Individuals wanted to feel confident about how their personal information was gathered, stored and used. It could be argued that this was the first indication of the nascent cyber security environment we know today.

The Government's response to the demand for privacy became our first milestone – the introduction of the Personal Information Protection and Electronic Documents Act (PIPEDA) which received Royal Assent on April 13, 2000.² PIPEDA was not a response to cyber attacks rather, it was concern about the collection, use and disclosure of

personal information. Canadians were demanding adequate privacy protection in a new digital economy. The law has applicability nationally with the exception of Alberta, British Columbia, and Quebec, or within Ontario relating to personal health information, as their privacy laws were deemed to be substantially similar to PIPEDA.

Canadians were demanding adequate privacy protection in a new digital economy.

While attention continued to be placed on the protection of personal information, there was mounting concern about increasing cyber attacks against government and business. The number of Canadians who were victims of identity theft was also rising. Nation states and cyber criminals were increasing their attacks in an effort to collect intellectual property. Concern was expressed about the vulnerability of Canada's critical infrastructure (CI) which is dependent on automated systems and interconnected networks. Attacks such as the ILOVEYOU virus, the Blaster worm, the Conflicker worm, the SQL Slammer worm, and the Stuxnet worm became the bane of cyber security defenders worldwide. The result was the second milestone, the establishment of a Cyber Security Task Force (CSTF) within Public Safety Canada in 2006.

The CSTF's mandate was to consult with the private sector and make recommendations on a cyber security strategy for Canada. The focus was to be on the management and control of cyber security risks, identifying CI interdependencies across sectors, and recommend mitigative measures.³ Simultaneously, Public Safety Canada continued to enhance the capability of its Canadian Cyber Incident Response Centre (CCIRC) which was responsible for providing cyber security mitigation strategies intended for government departments and agencies and the CI sector.⁴

Public Safety Canada subsequently produced the third milestone, Canada's Cyber Security Strategy in 2010 and related Action Plan 2010-2015 for Canada's Cyber Security Strategy.⁵ The Strategy was significant as it was the first time the Government had articulated the national importance of cyber security, and committed financial resources

to the implementation of the action plan. Much of the focus was on securing Government systems. Notable examples include establishment of the Cyber Threat Evaluation Centre in the Communications Security Establishment and Shared Services Canada's efforts to consolidate the Government's digital backbone and implement an enterprise approach for

the delivery of IT security services. The strategy also identified the need for partnering to secure vital cyber systems outside the federal Government and helping Canadians be secure online.

In the period following the release of the strategy, the cyber threat environment and technology evolved. The scale and nature of cyber crime mushroomed. Cyber attacks employing ransomware marked a significant change in how cyber crime was conducted.

Ransomware attacks became a victim equalizer. No longer were attackers only going after victims that possessed valuable intellectual property or huge financial resources. Attackers targeted data that only had value to the victim, where its loss, or inaccessibility, would severely impact a victim's operational capability. During the early years of ransomware attacks, victim's data was encrypted to make it unusable. Victims were willing to pay to have their data restored to enable their business to operate. Attack techniques evolved with attackers threatening to publicly release the victim's data or to sell it. During COVID, attackers focused on particularly vulnerable and critical organizations such as hospitals. The goal of the attackers was to create a sense of urgency and fear to incentivize payment of the ransom.

Criminal gangs began conducting cyber operations as a business. Advances in technology enhanced their capability while at the same time making it easier to become a criminal. Cyber attack tools became readily available online and relatively easy to use, even for the non-technical criminal.

Concurrently, some nation states permit cyber criminals to operate with limited intervention providing they followed a couple of rules – do not attack entities within their country and when called upon, conduct operations to support their nation's intelligence services. Identifying whether the attacker is a cyber criminal, or a nation state became increasingly difficult.

A milestone arose when foreign attackers successfully accessed Canadian government systems. In 2011, hackers using IP addresses from China infiltrated three Canadian



government departments, exfiltrating classified data. In 2014, the National Research Council of Canada (NRC) was the target of a cyberattack from a “highly sophisticated Chinese state-sponsored actor.”⁶

The 2010 Cyber Strategy included a review mechanism to assess its progress on improving Canada’s cyber resilience and to adjust as necessary. The subsequent 2017 Horizontal Evaluation of Canada’s Cyber Security Strategy led to the next milestone, the release of the 2018 National Cyber Security Strategy, and subsequent issuance of the National Cyber Security Action Plan (2019-2024). Three

The Centre became the country’s unified source of expert advice, guidance, services and support on cybersecurity.

goals were identified: focusing on secure and resilient systems, developing an innovative and adaptive cyber ecosystem, and providing effective leadership and collaboration.⁷

The National Strategy announced several subsequent milestones including the creation of two flagship organizations, the Canadian Centre for Cyber Security (CCCS) and the National Cybercrime Coordination Centre (NC3).

The launch of the CCCS (the Centre) marked a significant shift in the federal government’s effort to enhance the cyber resilience of the private sector. The Centre became the country’s unified source of expert advice, guidance, services and support on cybersecurity. While

the Centre retained responsibility for the security of federal government systems, it created programs designed specifically to assist the private sector. Using its extensive technical expertise, the Centre started producing technical guidance, issuing alerts about cyber threat actors, and, on a bi-annual basis, publishing a National Cyber Threat Assessment. This marked an advancement in the government’s efforts to assist the private sector to be aware of and cope with the increasingly hostile cyber threat environment.

As a National Police Service, NC3 provides an essential coordination function for all law enforcement investigations against cyber criminals. It also works with international partners to combat cyber crimes, which has become a key requirement as many cyber incidents have an international nexus. NC3 and law enforcement’s efforts are already becoming apparent with the conviction of major cyber criminals.⁸

Consumers and businesses also required protection from the misuse of digital technology including spam and other electronic threats. Canada’s anti-spam legislation (CASL) was created in 2014 to address this issue. Although designed to reduce the volume of spam received by Canadians, the legislation also dealt with other threats including identity theft, phishing and the spread of malicious software, such as viruses, worms and trojans (malware).⁹

2019 marked another significant milestone with the passage of the Communications Security Establishment Act. The Act was passed as part of the omnibus National Security Act 2017 that reformed the oversight on Canada's national security organizations. CSE acquired new tools in the defence against foreign cyber attackers. Authorization

Businesses realized that no organization can fully protect itself in this cyber threat environment—that a collaborative approach is required.

was given to CSE to conduct defensive cyber operations “to help protect systems of importance and federal institutions during major cyber incidents when cyber security measures alone are not enough”. CSE's 2023-2024 Annual Report revealed that its defensive cyber operations were used for the first time against a foreign ransomware group that was targeting multiple Canadian critical infrastructure organizations.¹⁰ Authority was also given for CSE to undertake active cyber operations to proactively disrupt foreign-based threats to Canada's international affairs, defence or security interests.

Canada's private sector also responded to the worsening cyber threat environment. Businesses realized that no organization can fully protect itself in this cyber threat environment – that a collaborative approach is required. The expression, ‘none of us are as smart as all of us’ characterized the call to action. The next milestone was the business community's establishing the Canadian Cyber Threat Exchange (CCTX). It became Canada's cross sector centre for collaboration through sharing cyber threat information, best practices and experiences.

Establishment of the CCTX represented a shift in the concept of cyber security. Cyber security was no longer seen as

a competitive advantage. To mitigate this growing business risk, all businesses need to have an understanding of the cyber threat environment which is enabled through sharing and collaboration. Competition is left to the provisioning of goods and services. Businesses also began reevaluating their corporate governance of cyber security. There was a growing realization that cyber security had become a whole of business issue. Cyber moved out of the shadows and was no longer the sole domain and understanding of technical experts. Cyber resilience was recognized as a matter of assessing and managing this business risk. Like business continuity planning, this is the responsibility of business units. Overall, these changes represented a shift from the concept of cyber security to one of cyber resilience. Businesses need to be aware of, and prepare for, cyber attacks and subsequently plan for incident response and business recovery. The assumption has now shifted to a recognition that the business will be the scope of a successful cyber attack.

Meanwhile, international attention continued to be given to the increasing cyber threat, and the parallel need to protect personal data. There was a realization that data privacy and security were convening; it's not possible to have one without the other. Canadian businesses are impacted by these efforts, e.g., by legislation such as the European Union's rules and legislation on data protection, including the 2016 General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive.¹¹ Action is also underway to counter the growing number of ransomware attacks.

For example, the United States organized what has become known as the International Counter Ransomware Initiative (CRI) with 68 members, including Canada. CRI is working to build resilience against ransomware attacks and leverage the ecosystem to disrupt the ransomware criminal industry. These efforts seek to “undercut the business model that underpins the ransomware ecosystem by driving forward work on secure software and labeling, methods to counter the use of virtual assets as part of the ransomware business model, policies to reduce ransom payments, increase and improve reporting, cyber insurance, and a playbook to guide businesses on how to prepare for, deal with, and recover from a ransomware attack.”¹²

The United States and Canada recognized that they have a shared physical border and a shared infrastructure and that a coordinated approach to cyber security is required. Consequently, in 2022, Public Safety Canada and the Department of Homeland Security established a Cyber Security Action Plan. Elements of the Plan include enhancing incident management collaboration, joint engagement

and information sharing with the private sector on cyber security and continued cooperation on ongoing cyber security public awareness efforts.¹³

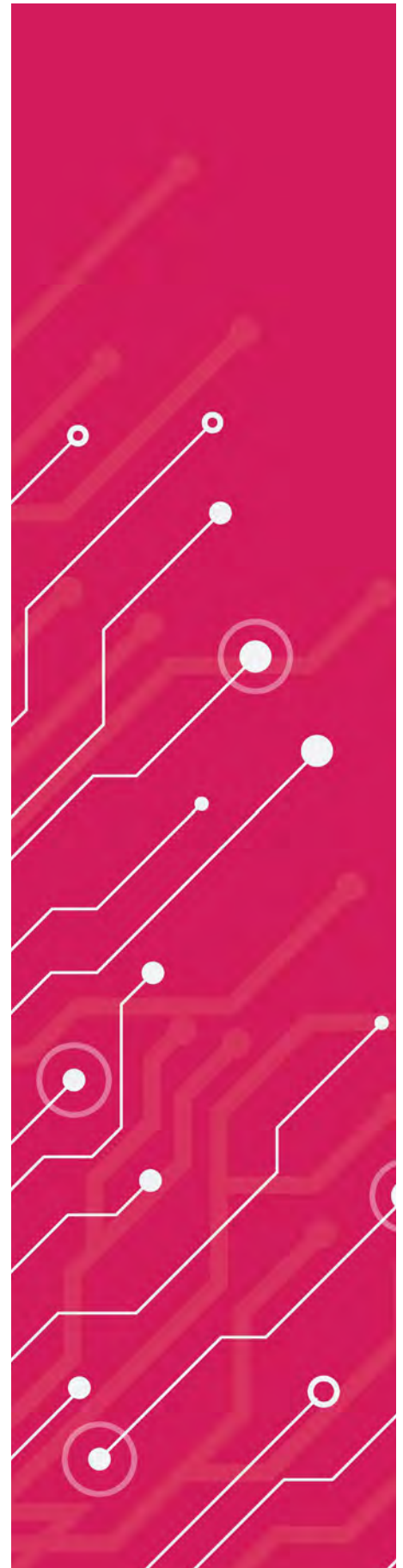
The cyber threat environment has not diminished. Attacks are becoming more sophisticated and the costs associated with successful breaches are mounting. Ransomware attacks remain a persistent threat. Nation states are increasing their cyber attacks, going beyond traditional espionage, seeking commercial advantage by stealing intellectual property for the benefit of their domestic industries. They are also prepositioning themselves in critical infrastructure for use at a time of their choosing, e.g., during a crisis.¹⁴

The technology environment is also changing. Advances in machine learning combined with generative artificial intelligence (AI) have enhanced the ability of cyber attackers. Also, while AI is also proving to be a useful tool for cyber defenders, it fails to neutralize the benefits to the attackers. The drive to create quantum computing is accelerating. Businesses now need to consider the immediate implementation of quantum resistant cryptography to defend themselves against the phenomenon of ‘collect now and decrypt later.’

In response to the risk environment, the Canadian government introduced two additional legislative milestones, the *Cyber Security Act* (Bill C-26) and *Countering Foreign Interference Act* (Bill C-70). The former is being considered by the Senate and the latter received Royal Assent in June 2024. Both implicate the private sector. The *Cyber Security Act* includes mandatory reporting requirements of cyber security incidents by designated CI operators. They need to establish and implement cyber security programs and mitigate supply-chain and third-party risks. Designated operators are those falling within the legislative authority of Parliament, e.g. telecommunications services, interprovincial or international pipeline and powerline systems, nuclear energy systems, banking and clearing and settlement systems and some transportation systems.¹⁵ The *Foreign Interference Act* provides the *Canadian Security Intelligence Service* the ability to provide threat information to the private sector, something that has been sought by the private sector but formerly not allowed.

In this rapidly changing cyber threat environment, some immediate positive milestones are required: an updated national cyber security strategy, passage of Bill C-26, and updating PIPEDA. Going forward, governments, businesses, and academia will continue their efforts to create new milestones, enabling Canada to demonstrate leadership both nationally and internationally. @

Robert (Bob) Gordon is the Executive Director of the Canadian Cyber Threat Exchange (CCTX). Prior to joining the CCTX, Bob held several senior leadership roles in the private and public sectors. Most recently, Bob was a Director, Global Cyber Security at CGI. Prior to this, he enjoyed a long and successful career in the Federal Government, which included being the architect of Canada’s first Cyber Security Strategy for which he received the Deputy Minister’s Achievement Award.





Facing the Cyber Storm: Canada's Path to Building Resilience in 2025

by [J. Paul Haynes](#)

In 2025, Canadian organizations are facing a perfect storm of escalating cyber threats, impacting sectors as varied as healthcare, finance, energy, and technology. From increasingly sophisticated ransomware attacks to state-sponsored espionage, the cyber threat landscape is now more complex and dangerous than ever before.

Canadian companies—particularly small and mid-sized businesses (SMBs)—are especially vulnerable due to under-resourced security measures and limited threat intelligence capabilities.

At the same time, ransomware attacks targeting critical supply chains have highlighted vulnerabilities that ripple across entire sectors, underscoring the need for a united approach.

By identifying the top three emerging cyber threats in 2025, Canadian organizations can better assess their preparedness against these threats, particularly ransomware, which has become the most pervasive and costly type of cybercrime.

Moreover, as cyber threats rise in complexity, it's clear that the Canadian government must collaborate with businesses to protect Canada's digital future. This may occur through creating robust cybersecurity policies, taking recommendations from Canada's top cyber experts, building cross-sector partnerships, and fuelling the cybersecurity talent pipeline.

Top 3 Emerging Cybersecurity Threats Impacting Canadian Businesses in 2025

1. RANSOMWARE AS A SERVICE (RAAS) AND SUPPLY CHAIN INFILTRATION

The evolution of ransomware has ushered in a new era of Ransomware-as-a-Service (RaaS), a business model that enables expert cybercriminals to research and develop new ransomware campaigns and sell, or rent, them to amateur hackers.

This trend has empowered threat actors, allowing them to target SMBs and enterprise organizations, especially within critical infrastructure and supply chains, with alarming efficiency.

Despite some progress, most Canadian organizations – especially SMBs – are unprepared for sophisticated ransomware attacks. Lack of budget, expertise, and access to advanced cybersecurity services leaves SMBs highly vulnerable.

On the other hand, while larger enterprises may have greater resources, they remain exposed due to expansive attack surfaces and the vast complexity of their supply chains, where smaller, less-secure vendors become weak links.

To combat ransomware and mitigate supply chain risks, the Canadian government must play a proactive role in bolstering defenses. For one, given the critical role that 24/7 threat detection and response capabilities play in a multi-layered cyber defense strategy, the Canadian government should consider providing some financial incentives that encourage Canadian businesses to partner with local Managed Detection and Response (MDR) providers.

As a July 2024 Centre for International Governance Innovation (CIGI) policy report points out, these partnerships will offer SMBs a practical defense by providing critical monitoring and response capabilities that are otherwise unaffordable.

2. RANSOMWARE AND STATE-SPONSORED ADVANCED PERSISTENT THREATS (APTs) ACTIVITY

Canada’s critical infrastructure is increasingly under attack from ransomware groups and state-sponsored actors,

including Advanced Persistent Threats (APTs), which exploit Canada’s cybersecurity weaknesses to support espionage and disrupt our economy.

Sophisticated state-sponsored threat actor groups from Iran, North Korea, Russia, and China use varied methods to gain initial access to organizations including, phishing, exploiting known vulnerabilities, and zero-day exploits to infiltrate corporate networks, where they can siphon sensitive data and positioning themselves for potential sabotage.

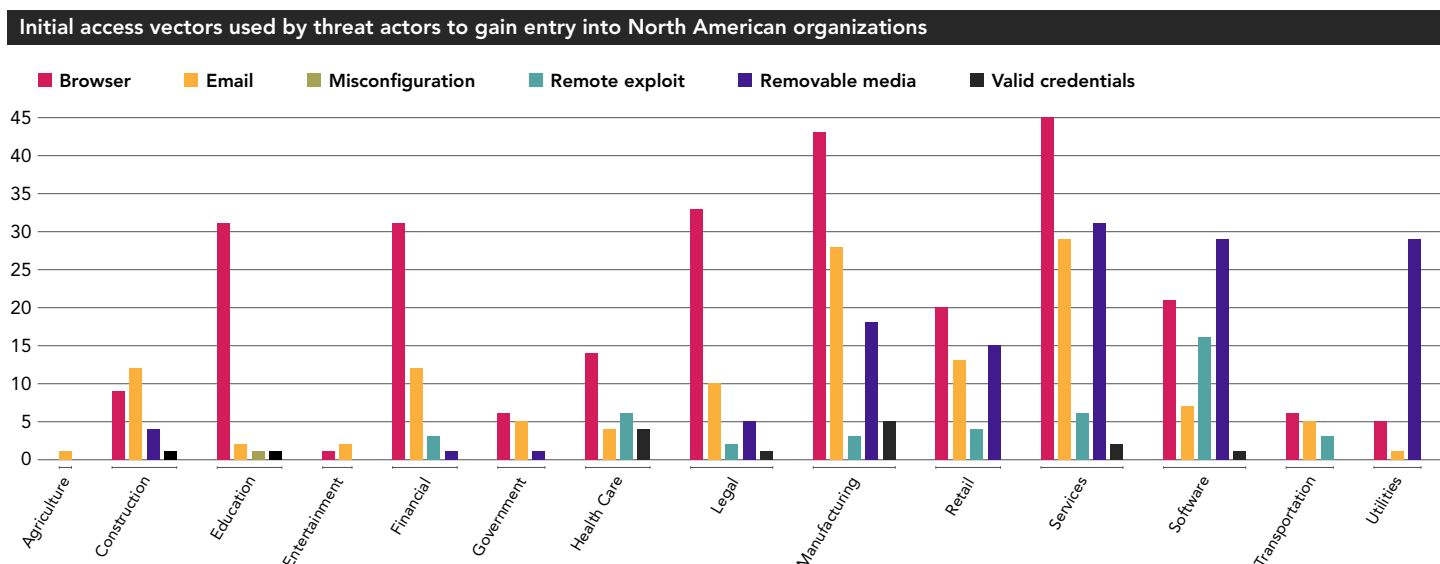
As stated in the Canadian Centre for Cyber Security’s National Cyber Threat Assessment 2023, and again in the National Cyber Threat Assessment in 2024, the impact of these state-sponsored attacks goes beyond financial loss, posing a strategic risk to Canada’s national security and sovereignty. Unfortunately, given that many Canadian organizations lack real-time threat response tools and threat intelligence resources to counter APT tactics, they remain highly susceptible to infiltration.

To counter ransomware groups and state-sponsored cyber threats, the Canadian government should develop and foster a centralized, collaborative approach that mirrors the U.S. Joint Cyber Defense Collaborative (JCDC).

As part of this initiative, Canadian MDR providers can work with the government as well as national defense and intelligence agencies to get the appropriate security clearances and conduct coordinated responses to APT activity.

3. USE OF DRIVE-BY SOCIAL ENGINEERING TACTICS FOR BROWSER-BASED THREATS

Threat research from eSentire’s Threat Response Unit (TRU) has shown threat actors are increasingly using fake browser



updates to lure employees into downloading malware and to gain initial access into an organization's environment.

In addition, cybercriminals are also using drive-by social engineering tactics, such as search engine optimization (SEO) poisoning to lure employees searching for common documents like legal forms or invoicing templates into downloading the GootLoader and SolarMarker malware. Once they have gained access, attackers can perform reconnaissance, exfiltrate data, and deploy ransomware, often without detection.

What's more, the threat trend data observed by eSentire's TRU team shows that browser-based attacks now represent 70% of all threats seen in our global customer base.

By fostering a "whole-of-society" approach, the Canadian government would ensure that cyber resilience extends across all sectors.

To protect against browser-based attacks, the Canadian government may consider providing subsidies to support advanced endpoint protection (EDR) and advocating for regular security awareness training for all employees. Moreover, funding incident response tabletop exercises that simulate social engineering attacks can further strengthen preparedness across Canadian businesses.

Key Recommendations to Bolster Canada's Cybersecurity Posture

A. DOMESTIC MDR INCENTIVES

To meaningfully improve Canada's cyber resilience, government-led incentives that prioritize the use of Canadian MDR providers are essential. By providing 24/7 monitoring, rapid detection, and expert-led incident response, MDR firms offer a vital service in the fight against ransomware and other advanced cyber threats, especially for SMBs that often lack in-house cybersecurity capabilities.

Furthermore, Canadian MDR providers bring local expertise and familiarity with the unique regulatory, threat, and business environments of Canada, making them highly relevant to addressing the specific needs of Canadian organizations.

Unfortunately, the costs associated with implementing a comprehensive cybersecurity strategy can be restrictive for many Canadian SMBs, and this is where government incentives could bridge the gap. By offering non-refundable tax credits or direct subsidies for Canadian businesses that partner with domestic MDR providers, the government can encourage broader adoption of critical cybersecurity services.

These incentives would make MDR services more accessible to SMBs, helping them benefit from real-time threat detection and response, 24/7 SOC-as-a-Service, and proactive threat intelligence and threat hunting services that may otherwise be beyond their financial reach.

This would empower SMBs to respond to ransomware and other cyber incidents with the same efficiency as larger enterprises, protecting their operations and reinforcing Canada's economic stability in the face of cyber threats.

B. ESTABLISHING A NATIONAL CYBER DEFENSE COLLABORATIVE

In 2021, the Cybersecurity and Infrastructure Security Agency (CISA) launched the [U.S. Joint Cyber Defense Collaborative \(JCDC\)](#), creating a platform for real-time intelligence sharing, uniting public and private sectors to prevent, detect, and respond to cyber incidents on a national scale.

By leveraging the expertise and intelligence of private cybersecurity firms alongside government resources, the JCDC has accelerated the U.S.'s response to ransomware and other high-profile cyber threats.

Adopting a similar framework in Canada would create a centralized defense mechanism, enabling faster information sharing, coordinated responses, and policy alignment across sectors. Under this collaborative model, Canadian MDR providers and cybersecurity firms would act as strategic partners to government agencies, ensuring that actionable threat intelligence is disseminated quickly and securely to those on the front lines of cyber defense.

This approach would unify the cybersecurity efforts of Canadian private companies and public entities, creating a robust, national cyber defense ecosystem.

By fostering a "whole-of-society" approach, the Canadian government would ensure that cyber resilience extends across all sectors, from large enterprises to SMBs. This initiative would enable more robust responses to ransomware by coordinating private and public resources, reducing the impact of attacks on Canadian businesses, critical infrastructure, and government systems alike.



A collaborative defense model would also facilitate the creation of standardized best practices and incident response protocols that private companies could adopt, enhancing the security posture across all industries.

C. ADDRESSING THE CYBERSECURITY SKILLS GAP

Canada, like its North American and European peers, is currently facing a significant cybersecurity skills shortage. In fact, according to the Information and Communications Technology Council (ICTC), one in six positions in cybersecurity remain unfilled in Canada.

This skills gap presents a critical barrier to improving national resilience against ransomware and other cyber threats; it not only impacts operational security but also puts Canada at a disadvantage in defending against sophisticated cyber threats that require specialized expertise.

The Canadian government has a unique opportunity to address this skills gap by supporting training incentives and subsidies for cybersecurity education and certifications. By providing tax credits to companies investing in their cybersecurity workforce, the government could promote ongoing professional development, offsetting the high costs associated with industry-standard certifications and training programs.

With financial incentives, Canadian organizations can afford to train more specialists, contributing to a stronger, more competitive cybersecurity workforce that benefits the entire Canadian economy.

Beyond subsidies, the government could also consider partnerships with academic institutions and private sector firms to create specialized training programs and apprenticeships,

particularly for entry-level cybersecurity roles. These programs would attract new talent into the cybersecurity field and provide hands-on experience, allowing trainees to work with experienced MDR providers to develop practical skills.

All in all, addressing the cybersecurity skills shortage is crucial to reducing Canada's vulnerability to ransomware and other cyber threats, and it is one of the most effective long-term investments the government can make in the nation's digital security infrastructure.

As we look to the future, one thing is clear: protecting Canada's economic stability and digital sovereignty requires a proactive, unified approach.

The rising tide of ransomware, state-sponsored espionage, and sophisticated malware requires a whole-of-society approach to defense, one that prioritizes local partnerships, government support, and continuous collaboration.

Canada's cyber resilience depends on decisive action from both public and private sectors. To secure Canada's digital future, policymakers must act swiftly to foster an environment where businesses, cybersecurity providers, and government agencies work together to combat evolving threats. ⁸

J. Paul Haynes is the President and Chief Operating Officer at eSentire. In his role, he oversees all security operations and customer success functions and leads the Corporate Development team. J. Paul is a professional engineer with a 25-year entrepreneurial track record of success. His business acumen, in-depth understanding of technology, and strong leadership have made him a respected and reliable voice on the topic of cybersecurity in North America and Europe.



Securing Digital Frontiers: Tackling Cybersecurity and Privacy Challenges in 2025

by [Michael Argast](#)

2024 saw an explosion in the adoption of industry frameworks and increase in government regulations in cybersecurity and privacy domains. The reason is simple—widespread adoption of cloud, SaaS, AI and interconnections of networks and data in business are dramatically increasing the data spread and risk for most organizations. Despite increased investments in cybersecurity, breaches and data losses reached unprecedented levels in 2024, underscoring critical gaps in existing measures.

Here are some highlights of this trend *just* in 2024.

Regulatory Updates:

- **DoD finalizes CMMC rule**—this will lead to most DoD suppliers having to achieve this standard
- **DORA** implements cybersecurity resiliency requirements in EU sold products with “digital elements”
- **NIS2** is now the first EU wide law on cybersecurity
- **Continued fall-out** over the demise of the EU-US Privacy Shield

- **Texas TX-Ramp** now in place for Texas public sector purchasing
- **Compliance automation** market leader **Vanta raises** \$150M USD at \$2.45B valuation
- **Everybody is trying** to regulate AI and come up with standards
- **New privacy regulations** in Delaware, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Washington and Texas
- **NIST finally adds** Governance to CSF V2
- **FTC continues to step up** enforcement, FBI successfully prosecutes Uber CISO for concealing breach information
- **Third-party breaches** accounted for 29% of incidents in 2024, highlighting the critical need for robust vendor risk management systems.

Notable incidents and fines:

- **Change Healthcare's ransomware** attack took down much of the US healthcare payments system
- **Infosys McCamish's incident** resulted in losses at Bank of America
- **AMEX suffered a card detail** compromise from a merchant processor
- **The Okta breach continues** to cause fallout and downstream issues
- **Snowflake customers were hit** by targeted account compromises
- **Lehigh Valley Health Network** agreed to a \$65M settlement over nude cancer scans
- **23andMe suffered a massive** breach and paid \$30M
- **AT&T got hit once again** for a \$13M fine by the FTC.

What do you need to do?

FOUNDERS

Identify if your company idea is in a space that may require compliance with one or more standards in order to sell to your addressable market. Of particular importance to companies working with sensitive information (PII/PHI) in regulated industries (health, finance, defence, government).

SMALL

Pre-revenue to \$25M annually: If you work with 3rd party data, you need to plan to implement minimum security controls and standards (SOC2). SaaS/Healthtech/Fintech/etc. Do this leveraging tools and service providers to help you keep costs down while putting core requirements in place. Why: Otherwise you shouldn't expect to be able to sell to medium/larger enterprises or government clients.

MEDIUM

\$25M-\$100M annually: You need to start considering scaling your investments and addressing multiple frameworks. Ensure you have plans to address privacy and regulations, and bake these into your product/service development process. Fines get to be >\$1M at this scale. You should be looking closely at 3rd party risk management—especially at smaller vendors. Solutions like trust pages and security questionnaire automation become high return investments at this scale. You may be operating in multiple geographies, so being aware of local variations like UK Cyber Essentials, DORA, NIS2 in EU, CPRA in California, becomes important.

LARGER

\$100M annually: You become an interesting target for regulators. Public companies need to be aware of FTC rules, ITGC controls under SOX. You should have someone on your board who has responsibility for and competency in cybersecurity and enterprise risk management. In extreme cases rules can call for jail time for CISOs/executives who've shown gross negligence in security matters—in practice this has mostly related to failure to disclose breach information where required by law.

Selecting technology and service partners

TECHNOLOGIES SHOULD AT A MINIMUM:

1. **Provide you the ability** to automate a wide range of evidence collection—critical as you scale standards, but saves tons of effort and makes it possible to achieve compliance for smaller firms. Look for key API integrations into areas like your Identity Provider, cloud stack, HRIS, MDM and key SaaS platforms. Also look for ability to pull in asset inventory and compliance posture.
2. **Make it easy for auditors** to conduct work without requiring manual evidence sharing. Look for a large number of integrated audit partners and make sure your selected auditor will actually use the platforms (this will save you time, effort and money).

It is critical for businesses of all sizes to recognize the impending tidal wave of security demands.

ADDITIONALLY, MEDIUM AND LARGER FIRMS WILL BENEFIT FROM ADVANCED CAPABILITIES:

- 1. Manage key workflows** like risk assessments, employee onboarding and off boarding, access reviews, vendor risk management.
- 2. Provide cross-mapping** of controls across multiple frameworks, collecting of custom controls/evidence, assigning control owners and sending notifications of out of compliance controls
- 3. Easily share information** on your security posture with clients via tools like Trust Centers/Pages, automate security questionnaire responses

PARTNERS SHOULD:

- 1. Be deeply versed in the tool** you select to work with—not just have generic security expertise
- 2. Expertise in ISO27001/SOC2** and other relevant compliance standards
- 3. Be able to provide a wide range** of compliance related services or a partner ecosystem—platform experience (as noted), pen testing, privacy support, audit partners, managed threat detection, awareness training, policy writing, vCISOs experienced in compliance, supporting security questionnaires, vendor risk assessments, background checks, etc. etc. More experienced partners will have packages specifically for compliance and security programs, less experienced providers will focus on hourly based billing models.
- 4. Have a background** in your particular industry or sector—B2B SaaS, health, financial, etc.

What about AI?

No conversation about security, compliance and regulation in 2024 could be complete without addressing the topic of AI. AI has a number of key impacts that every business should consider:

- 1. Threat actors Leveraging AI**—enabling more sophisticated social engineering and other forms of attacks, invalidating traditional voice and video based verification techniques
- 2. Security for LLM models**—testing and securing models against in-the-wild techniques like prompt injection attacks, data poisoning, bias scenarios, denial of service attacks and more
- 3. Governance and Privacy Challenges** in AI
Adoption—change in vendor behaviours in data usage for training purposes, updating data processing agreements, implementation of AI features in pre-existing products, auto opt-in on privacy policy changes involving AI, data harvesting
- 4. Data integrity/trustworthiness issues** related to AI—hallucinations, quality control on AI chatbots and customer experience challenges, adoption speed vs. test case verification

In conclusion

Given the continued challenges, it is critical for businesses of all sizes to recognize the impending tidal wave of security demands from customers, partners, investors and regulators and incorporate plans to address these into their business strategies. Selecting automation tools, partnering with services firms who specialize in security and privacy compliance standards, baking certifications and regulations into your product development and business strategies—these steps will allow you to stay ahead of the rising tide and build a resilient business in the years to come.

By proactively integrating compliance and security measures into their strategic plans, organizations can not only mitigate risks but also gain a competitive edge in an increasingly regulated digital economy. 🌊

[Michael Argast](#) is Co-founder and CEO at Kobalt.io based out of Vancouver, BC. As the co-founder and CEO of Kobalt.io, Michael has over five years of experience in providing cyber security programs that address the needs of small and mid-sized organizations.



The State of AI in Canada

by [Helen Oakley](#)

Introduction

Artificial intelligence (AI) is revolutionizing industries and reshaping operations worldwide. In Canada, AI is recognized as a catalyst for economic growth, with transformative potential in sectors like healthcare, finance, manufacturing, and cybersecurity. Significant federal and provincial investments underline the country's commitment to fostering innovation and addressing adoption challenges.

Globally, trends such as generative AI, platform engineering, and autonomous systems are shaping the AI landscape. Canada's strong foundation in AI research and talent development positions it well to capitalize on these trends.

However, balancing opportunities with risks such as cybersecurity vulnerabilities and governance challenges remains critical to unlocking AI's full potential.

Adoption Trends and Industry Efforts

AI adoption in Canada is advancing, with notable variations across industries. As of late 2023, 37% of large enterprises reported AI use, up from 34% earlier that year. Finance, healthcare, and technology sectors lead adoption, leveraging AI for applications such as fraud detection and personalized healthcare solutions. In contrast, manufacturing and retail face barriers like high costs and skill shortages.

The federal government's \$2.4 billion initiative and provincial programs in Ontario, Quebec, and British Columbia drive adoption and innovation. Initiatives such as the [Pan-Canadian AI Strategy](#) and the [Artificial Intelligence and Data Act \(AIDA\)](#) aim to create a supportive ecosystem. International frameworks like the [NIST AI Risk Management Framework](#) and [AI Integrity and Safe Use Foundation \(AISUF framework\)](#) also guide responsible AI integration.

The transformative potential of AI comes with significant risks that demand careful oversight.

Despite progress, concerns over data privacy, security, and workforce readiness persist. Addressing these challenges is essential for Canada to maintain its global competitiveness and fully realize AI's transformative potential.

Technological Trends

AI technologies are advancing rapidly, transforming industries through key trends such as generative AI, cybersecurity innovations, and platform engineering.

GENERATIVE AI AND AGENTIC SYSTEMS

Generative AI combines creativity and autonomy, driving innovations in areas like fraud detection, personalized marketing, and inventory management. Advancements in agentic AI and multi-agent systems (MAS) enhance this autonomy. These systems independently perform complex tasks and collaborate toward shared goals, offering solutions in supply chain management and smart cities. Together, they signal a shift toward more autonomous and collaborative AI applications.

CYBERSECURITY INNOVATIONS

AI-driven systems transform cybersecurity by enabling continuous threat detection and adaptive responses. Tools like [PentestGPT](#) automate vulnerability assessments, enhancing defenses for both traditional and AI systems. For critical

infrastructure, AI supports predictive maintenance and resilience, underscoring the need for robust frameworks to mitigate risks.

PLATFORM ENGINEERING AND GOVERNANCE

Platform engineering simplifies AI integration, enabling businesses, including smaller enterprises, to adopt AI without extensive expertise. Emerging AI governance platforms address ethical and regulatory needs by offering tools for monitoring, auditing, and risk mitigation. By aligning technological advancements with ethical considerations, these trends foster trust and accountability in AI systems.

Regulations for AI in Canada and Beyond

AI regulation is a global priority as governments address its rapid growth and associated risks. Canada's proposed [Artificial Intelligence and Data Act \(AIDA\)](#) governs high-impact AI systems in critical sectors like healthcare and law enforcement, emphasizing risk management, transparency, and accountability. Businesses must prepare for compliance by adopting robust governance frameworks.

Internationally, the [EU AI Act](#) enforces stringent, risk-based regulations for high-risk systems, while the U.S. takes a flexible approach with initiatives like the [National AI Initiative Act](#) and evolving state-level laws in regions such as California, Texas, and Colorado. Globally, nations like Japan and Singapore focus on voluntary standards emphasizing transparency and accountability. Canada contributes to this alignment through initiatives like the [Global Partnership on Artificial Intelligence \(GPAI\)](#) and the [Canada–France Declaration](#), ensuring ethical AI standards and fostering innovation.

Risks and Implications of AI

The transformative potential of AI comes with significant risks that demand careful oversight. For businesses, reliance on AI for decision-making can introduce vulnerabilities such as algorithmic biases, data breaches, and adversarial attacks. Governments face the challenge of ensuring that AI systems used in public services are fair, secure, and aligned with societal values while maintaining public trust.

For individuals, concerns about data privacy and the misuse of AI remain paramount. The use of AI in surveillance raises complex questions about balancing security needs with civil liberties. Additionally, the rise of agentic AI, which refers to highly autonomous systems capable of operating with minimal human oversight, brings ethical concerns around accountability and control. These concerns are

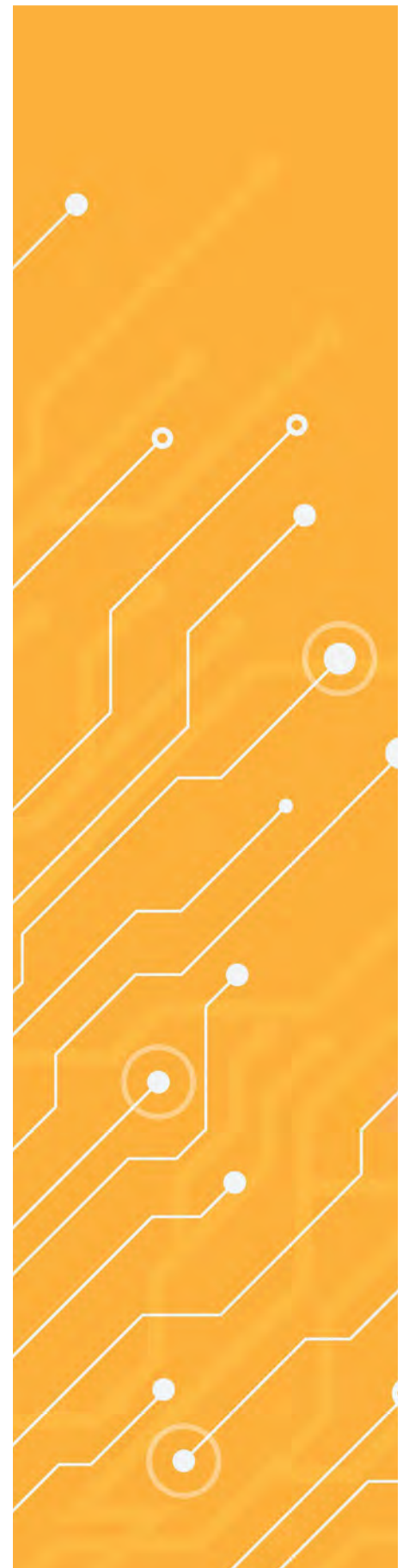
especially relevant when such systems influence critical decisions or operate in high-stakes environments.

To illustrate the diverse risks associated with AI adoption, the table below categorizes key challenges, highlighting their primary impacts and real-world examples:

Risk Name	Category	Primary Impact	Examples
Misinformation and Erosion of Trust	Misinformation	Degradation of information ecosystems, loss of shared reality, and reduced societal trust.	AI-generated misinformation, clickbait headlines, and manipulation in advertising ecosystems.
Diffusion of Responsibility	Governance Failure	Lack of accountability in societal-scale harm, leading to systemic biases and inequalities.	Automated hiring decisions or legal judgments influenced by AI with unclear accountability.
Inaccurate AI Outputs	Technological Weakness	Creation of unreliable, misleading, or incorrect results, reducing trust in AI systems.	LLMs generating hallucinated responses or incorrect outputs due to training limitations.
Entrenched Biases and Ideologies	Fairness	Amplification of biases, fragmentation of societal knowledge, and reduced political engagement.	AI assistants reinforcing user preferences and biases, hindering balanced decision-making.
Privacy Violations	Privacy and Security	Misuse of personal data, undermining trust and leading to potential exploitation.	Analysis of sensitive personal data without consent, enabling unauthorized surveillance.
Environmental and Societal Costs	Socioeconomic and Environmental	Strain on energy resources, societal disruptions, and growing resource inequalities.	High energy demands for training AI models impacting sustainability efforts.

This table is not exhaustive but highlights critical risks and their implications. Certain risks, such as misinformation, intersect with multiple categories, including fairness and technological weaknesses, illustrating the complexity of AI risk management. For a more detailed and exhaustive list of AI risks, resources such as the [AI Risk Repository](#) and [MITRE ATLAS](#) provide comprehensive insights and frameworks. These overlaps underline the importance of adopting holistic approaches to AI governance.

Effectively addressing these risks requires collaboration among businesses, governments, and civil society. By prioritizing transparency, accountability, and fairness in AI systems, stakeholders can mitigate potential harms while fostering trust, innovation, and societal resilience.



Recommendations and Best Practices

To fully harness AI's transformative potential while addressing its risks, stakeholders must adopt a structured, collaborative approach.

FOR POLICYMAKERS

Policymakers should advance frameworks like AIDA, harmonizing them with international standards to strengthen governance. Incentives such as grants and tax credits for ethical AI research can drive adoption. Supporting initiatives like the AISUF framework helps businesses implement maturity-based measures, ensuring secure scaling and innovation. Engagement in international forums is essential to align regulations and share best practices.

FOR BUSINESSES

Businesses must build robust AI governance capabilities, starting with foundational measures like transparency, data privacy, and ethical principles. High-impact systems, especially in critical sectors, require advanced practices such as scenario-based testing, continuous monitoring, and incident response frameworks.

CISOs play a vital role in securing AI systems. Key considerations include:

- **Addressing AI-Specific Vulnerabilities:**
Proactively mitigate risks like adversarial attacks, data poisoning, and model drift through tailored risk management.
- **Ensuring Data Privacy:**
Prioritize compliance with data protection regulations and embed privacy-by-design principles into AI systems.
- **Promoting Ethical AI Use:**
Establish policies to prevent biases and enhance AI explainability with fairness audits and ethical standards.
- **Continuous Threat Monitoring:**
Use AI-driven tools for real-time anomaly detection and dynamic system monitoring.

Maturity models, such as the AISUF framework, aim to offer a structured approach to scale securely and foster innovation. Upskilling employees in AI, cybersecurity, and governance, along with partnerships with academia and industry, can address talent gaps and prepare organizations for evolving regulations and threats.

By aligning security with innovation, businesses can ensure AI adoption drives growth while maintaining trust and resilience.

FOR EDUCATORS

Educators play a vital role in preparing the workforce for AI-driven industries. Integrating AI ethics and applications into K-12 curricula builds foundational awareness, while post-secondary programs should emphasize governance, cybersecurity, and critical infrastructure. Collaborations with businesses for hands-on learning opportunities ensure alignment with industry needs and bridge talent gaps.

Building a Resilient AI Ecosystem


By fostering collaboration among policymakers, businesses, and educators, Canada can create a resilient AI ecosystem. Foundational requirements, such as transparency and compliance, provide a baseline for all stakeholders. For high-impact systems and critical infrastructure, applying advanced measures ensures resilience and public trust. This holistic approach will enable Canada to lead globally in AI governance, ensuring that AI supports growth, security, and equitable outcomes for all.

Conclusion

AI presents unparalleled opportunities for innovation and growth, but its adoption comes with challenges that must be carefully managed. Canada is uniquely positioned to lead in AI research, development, and application, thanks to its strong talent base, supportive policies, and ethical focus.

By addressing adoption barriers, mitigating risks, and fostering collaboration across sectors, Canada can ensure that AI becomes a force for good—enhancing economic prosperity, improving public services, and safeguarding cybersecurity in an increasingly digital world. The path forward requires vigilance, investment, and a shared commitment to ethical innovation. 🌐

Helen Oakley, CISSP, GPCS, GSTRT, recognized as one of the Top 20 Canadian Women in Cybersecurity, is a leader in cybersecurity and AI transparency. She co-leads and contributes to groundbreaking publications on AI and security for CISA.gov (AIBOM Tiger Team) and OWASPAI.org (Agentic AI Security initiative), shaping standards for transparency and security in the evolving AI landscape. As Director of Secure Software Supply Chains and Secure Development at SAP's Global Security and Cloud Compliance, she champions security-by-design across SAP's engineering teams.

A photograph of three people in a professional setting. On the left, a man with glasses and a beard is seen in profile, wearing a light-colored button-down shirt. In the center, a woman with her hair in a ponytail is smiling and looking towards the man on the right. She is wearing a light blue button-down shirt and a lanyard with an ID badge. On the right, a man with a beard and wavy hair is smiling back at her, wearing a textured grey sweater over a white shirt. The background is a dimly lit office with a screen displaying some data or charts.

At Mastercard, we're working to keep people, businesses and governments more secure as our digital ecosystem evolves

From AI-powered cybersecurity to biometric authentication, our technology continuously assesses the landscape for evolving threats. Our innovations help prevent fraud and financial crime before they happen, keeping people secure.

Our work doesn't stop there. Learn how we are mobilizing partners across public and private sectors to build trust, secure financial inclusion and pave the road to financial health.





Bridging the cybersecurity gaps: Preparing for change in 2025

Presented by Mastercard

Generative AI is transforming the cybersecurity and fraud landscape, offering advanced tools to combat digital threats, while enabling fraudsters to attack with unprecedented sophistication. For Canadian businesses—particularly small and medium-sized enterprises (SMEs) in sectors like retail, banking and forestry—this technological shift presents both a challenge and an opportunity.

As fraud evolves alongside the rapid growth of digital payments, it is essential for leading technology providers to support Canadian businesses in navigating this complex risk environment. By embracing generative AI and building a strategic, layered defence, SMEs can proactively prepare for change and strengthen the future of their cybersecurity.

The Growing Impact of Generative AI

Fraud has adapted to changing technologies, and generative AI is accelerating this shift. By leveraging generative AI, fraudsters can create sophisticated attacks using AI-generated phishing emails or synthetic identities, which are harder to detect. They also scale operations with generative AI, which is enabling automation of account takeovers, authorization of push payment fraud and BIN attacks with speed and precision.

What's even more disturbing is they can mimic human behaviour using tools that generate lifelike text, voice and even video, allowing them to impersonate legitimate users



convincingly. For instance, card-not present (CNP) fraud losses are estimated to reach \$28 billion 1 by 2026, a 40 per cent increase from 2023,¹ driven by the rise of digital transactions. Generative AI allows fraudsters to leverage compromised data to exploit these vulnerabilities at scale. However, the same technology offers fraud fighters a powerful tool to detect, predict and prevent attacks.

Preparing for Change: A Practical Framework

To combat rising threats, Canadian businesses can adopt a structured framework to integrate generative AI into their cybersecurity strategies.

1. ASSESS CURRENT MATURITY

Businesses must determine their readiness for generative AI:

- **Stage 1:** No generative AI strategies in place.
- **Stage 2:** Strategies exist but lack implementation.
- **Stage 3:** Vendor-led AI tools are deployed.
- **Stage 4:** Internal teams manage custom AI-driven solutions.

Today, most businesses fall somewhere between stage 1 and 2. For them, reliance on stage 3 provides an effective and scalable entry point to combat evolving threats without overwhelming internal resources.

2. MAP THREATS AND USE CASES

Businesses should map fraud risks across the transaction lifecycle:

- **Pre-transaction:** Synthetic identity fraud, CAPTCHA evasion and account takeovers.
- **Transaction:** Authorized push payment fraud, unauthorized payments and BIN attacks.
- **Post-transaction:** Payout fraud and chargeback abuse.

By understanding where fraud risks are highest, businesses can identify opportunities for generative AI solutions, such as:

- **Behavioural Biometrics:** Detecting identity fraud by analyzing user behaviour.
- **Anomaly Detection:** Identifying irregular transactions to flag fraud before it occurs.
- **Synthetic Identity Detection:** Recognizing AI-generated accounts at the pre-transaction stage.

3. PARTNER WITH TRUSTED VENDORS

Generative AI deployment does not require a fully in-house solution. Businesses can partner with industry leaders, leveraging tools such as Decision Intelligence Pro. This Mastercard generative AI-powered solution scans over 1 trillion data points to assess transaction risks in under 50 milliseconds.

Early modeling shows this technology improves fraud detection rates by up to 300 per cent in some instances. By working with trusted vendors, Canadian businesses can enhance fraud mitigation without significant upfront investments.

Addressing Challenges

Adopting advanced cybersecurity measures isn't without hurdles. Businesses must ensure regulatory compliance, by navigating adherence to Canadian data privacy laws, such as PIPEDA. Generative AI tools must be implemented with transparency and ethical oversight.

Technology alone cannot solve the challenges posed by generative AI-enabled fraud.

There is also a great challenge with data transparency, as the "black-box" nature of AI can complicate decision-making processes. Businesses should prioritize tools that provide explainability, ensuring accountability in fraud detection systems.

Most importantly, there must be internal alignment. Implementing generative AI solutions requires cross-functional collaboration, where fraud teams, IT departments and legal teams must align on objectives, risks and implementation strategies.



Building a Resilient Cybersecurity Culture

Technology alone cannot solve the challenges posed by generative AI-enabled fraud. A resilient cybersecurity culture requires:

1. EMPLOYEE TRAINING:

Tailored education helps staff identify AI-driven phishing attacks, fraudulent communications and irregular behaviours.

2. CLEAR COMMUNICATION:

Open dialogue across departments ensures a proactive approach to evolving threats.

3. METRICS AND KPIS:

Tracking key indicators like fraud losses, false positives and detection rates enables continuous improvement.

By fostering vigilance across the organization, businesses can strengthen their defenses while improving response times to emerging threats.

Bridging the Gaps

Generative AI has created a dynamic and complex risk environment for Canadian businesses. With its industry-leading AI solutions, Mastercard can help bridge critical cybersecurity gaps by:

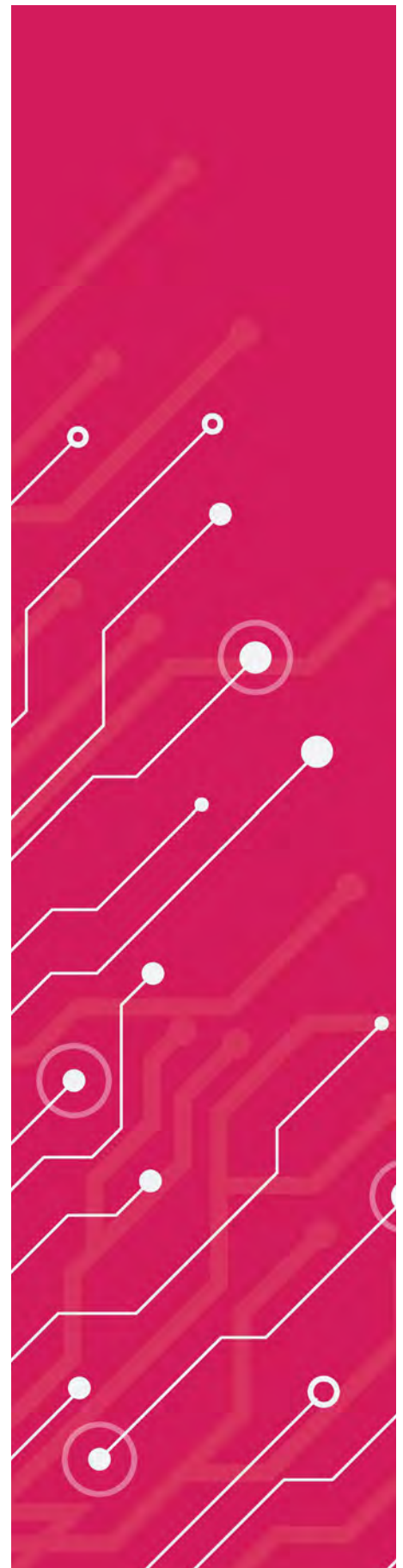
- enhancing fraud detection with tools like **Decision Intelligence Pro**, which improves real-time decisioning;
- supporting identity verification through behavioural biometrics and AI-driven risk scoring; and
- leveraging generative AI to monitor cyber risks and combat fraud throughout the transaction lifecycle.
- delivering actionable threat intelligence insights that help to classify malware types, identify threat actor relationships and recognize spear-phishing campaigns before they can impact business systems.

Generative AI is not just a tool for fraudsters—it is an opportunity for businesses to build smarter, more proactive defenses.

The rise of generative AI presents Canadian businesses with both a challenge and an opportunity. As fraudsters become more sophisticated, businesses must adapt to stay ahead. By assessing risks, partnering with trusted providers and fostering a resilient security culture, businesses can navigate the generative AI era confidently.

This article is based on “Generative AI: Preparing your fraud organization,” a whitepaper developed by Mastercard in collaboration with Glenbrook. For deeper insights and actionable strategies, visit mastercard.ca to access the full report.

¹ Datos Insights, July 2023.





Providing Cyber Security in Real Time

by [Paul Da Silva](#)

Introduction

Following the rise of cloud and cloud-native technologies (such as containers and Kubernetes), identities have increased both in number and complexity, and these changes pose a direct risk to enterprise security. According to the [2024 Trends in Securing Digital Identities](#) report from the Identity Defined Security Alliance (IDSA), identity-related breaches are on the rise, with 90% of organizations experiencing at least one identity-related incident in the past year, and 84% suffering a direct business impact as a result.

The increase in identities, and the increasing focus on identities by threat actors changes the dynamic for cybersecurity. Organizations need to adapt their methods for protecting sensitive identity data with new technologies because existing, on-premise security technology is just not capable of providing the level of identity security needed—especially in the cloud.

This article examines emerging cybersecurity disciplines and technologies and offers recommendations for organizations seeking to strengthen their Identity and Access

Management (IAM) strategies against evolving cyber threats in the cloud.

Why Traditional Cybersecurity No Longer Suffices

Traditionally, cybersecurity has been a scheduled and batched process:

- **Security updates, patches,** and system scans were scheduled at regular intervals (e.g., weekly, monthly) because primarily on-premise systems were relatively static and didn't require continuous maintenance.
- **Threat detection and** response involved collecting data over time and analyzing it in "batches" during specific timeframes, for instance after an incident or as part of routine audits, rather than in real time.
- **Vulnerability assessments,** compliance checks, incident response, and other security processes were performed manually and on a set schedule because organizations didn't need to adapt instantly to emerging threats.
- **Security policies and** configurations were static and, once established, only revisited during scheduled reviews rather than being dynamically adjusted to new risks or changes in the environment.

Modern threats evolve quickly, and modern cloud-native environments are dynamic, with workloads and identities that are changing constantly.

Scheduled processes are too slow and static for today's threat landscape, and the gaps created by delayed updates or periodic checks can allow threat actors to compromise environments.

Modern threats evolve quickly, and modern cloud-native environments are dynamic, with workloads and identities

that are changing constantly. Modern organizations can no longer rely on periodic snapshots or reactive measures. They need real-time, adaptive cybersecurity approaches that offer continuous monitoring and penetration testing, real-time analysis, real-time vulnerability assessment scans, real-time identification of identity security anomalies, and immediate responses.

Emerging Cybersecurity Disciplines: ITDR

Today, disciplines like Cloud Security Posture Management (CSPM) and Security Information and Event Management (SIEM) have achieved modern cybersecurity goals in the cloud. Other disciplines, like Identity Threat Detection and Response (ITDR), are just emerging in response to the explosion of distributed identities beyond the traditional network perimeter and the resulting increase in identity-related vulnerabilities and attacks. In fact, [Gartner recently labeled Identity Threat Detection and Response \(ITDR\)](#) as one of the top security and risk management trends.

ITDR refers to the combination of security tools and processes required to adequately defend identity-based systems. Gartner defines ITDR as "a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools, and processes to protect identity systems. It works by implementing detection mechanisms, investigating suspicious posture changes and activities, and responding to attacks to restore the integrity of the identity infrastructure."

The modern security challenges ITDR addresses include:

- **Real-Time Security Evolution**
Shifts identity protection from a periodic to a continuous process with behavioral analysis, event detection and investigation, and real-time mitigation of threats and non-compliant accounts.
- **Cloud-Native Identity Risks**
Addresses the dynamic nature of cloud identities in Kubernetes and hybrid environments.
- **Over-Permissioned and Stale Accounts**
Mitigates risks by discovering, identifying, and remediating over-privileged or inactive accounts.
- **Misconfigurations**
Proactively detects and corrects vulnerabilities in identity systems and configurations.

What are Some of the Top Emerging Technologies Powering ITDR?

- **Behavioral Analytics and Machine Learning (ML)**
Analyze user and entity behavior to detect deviations from normal activity. New developments include ML models trained to adapt to dynamic and containerized environments like Kubernetes.
- **Identity and Access Management (IAM) Integration**
Centralize visibility and control over hybrid identity systems like Active Directory, Entra ID, and Okta. Emerging IAM solutions support automated least-privilege policies in dynamic cloud environments.
- **Modern Privileged Access Management (PAM)**
Secure and monitor privileged accounts, enforcing zero trust principles across the identity lifecycle. Emerging PAM solutions address dynamic privilege needs in DevOps workflows and containerized environments.
- **Threat Intelligence and Automation technologies** use AI-powered automation to enforce security policies and respond to threats in real-time. New platforms integrate global threat intelligence feeds with identity-centric threat detection.

Tailoring ITDR to Critical Systems & Dynamic Environments: Kubernetes, Active Directory, and Entra ID

To effectively enhancing identity security across modern IT environments, organizations need to address the unique challenges of their specific platforms. Kubernetes, Active Directory, and Entra ID are foundational components of many organizations' identity and access ecosystems, and each presents distinct vulnerabilities and operational nuances.

ITDR offers tools and methodologies that can be adapted and tailored to mitigate the specific risks of these systems, enforce least-privilege access, and maintain a robust security posture in real-time.

ITDR and Kubernetes Identity and Entitlements Management (KIEM)

Kubernetes environments present significant security challenges, particularly around Role-Based Access Control (RBAC). RBAC in Kubernetes allows administrators to set granular permissions for resources, like pods and deployments. However, managing these permissions is complex, and misconfigurations, excessive privileges, and outdated

cluster versions are common, leaving organizations vulnerable to identity-based threats.

ITDR OFFERS ADVANCED TOOLS AND FEATURES THAT CAN HELP IDENTIFY RBAC ATTACKS:

- **Risk scoring** evaluates the security posture of identities by combining insights from runtime data, cloud misconfigurations, and container vulnerabilities. This holistic approach helps prioritize threats and streamline remediation efforts.
- **Admission controllers** enforce policies that align with the principle of least privilege. By doing so, they prevent unauthorized users or services from accessing sensitive resources.
- **Access audit logs** make it easier to investigate failed or suspicious login attempts. Regular reviews of stale or inactive identities further reduce the risk of unused accounts becoming attack vectors.
- The recent introduction of **Common Expression Language (CEL)** in Kubernetes version 1.30 further expanded ITDR's capabilities. CEL simplifies policy validation and enforcement, offering an alternative to traditional webhooks. This feature not only reduces complexity but also supports integration with CI/CD pipelines and GitOps workflows, ensuring security policies are consistently applied throughout the development lifecycle.

ITDR and Active Directory (AD)

Microsoft released Active Directory with Windows Server Edition in 2000, and it is still the main directory in use by organizations worldwide. With such widespread use, it is often a target for attackers who aim to take control of the directory and deploy ransomware or exfiltrate sensitive data.

AD's legacy nature makes it susceptible to misconfigurations and credential misuse, which can lead to unauthorized access, privilege escalation, and domain-wide compromises.

ITDR ADDRESSES THESE RISKS WITH:

- **Event Monitoring**
Collecting and analyzing security logs, metadata, and access control lists (ACLs) to identify unusual activity and detect misconfigurations.
- **Active Directory Certificate Services (ADCS)**
Proactively uncovering vulnerabilities in certificate management that attackers could exploit for privilege escalation.

- **Privilege Management**

Tracking privileged accounts and ensuring least-privilege principles are applied to prevent unauthorized access to sensitive resources.

- **Incident Response**

Providing detailed visibility into events, such as failed authentications or unauthorized privilege escalations, to streamline threat investigation and remediation.

ITDR and Entra ID (Azure AD)

Entra ID (formerly Azure AD) is a cloud-native identity provider critical to securing access to modern cloud applications and services. As a cloud-native environment, it requires dynamic and context-aware threat detection.

ITDR ENHANCES ENTRA ID SECURITY BY:

- **Role and Scope Management**

Monitoring role assignments and ensuring strict adherence to least-privilege principles.

- **Conditional Access Integration**

Enforcing dynamic access controls based on user behavior, location, and risk factors to minimize attack surfaces.

- **Privilege Escalation Mitigation**

Detecting and responding to attempts to misuse role assignments or administrative privileges.

- **Continuous Assessment**

Evaluating identity security posture in real-time to identify and remediate risks across cloud services and applications.

Conclusion: Moving from Legacy to Real-Time Security

For organizations to withstand the onslaught of modern identity-based attacks, transitioning from scheduled, legacy security models to real-time, adaptive disciplines like ITDR is essential. To make this transition successful, consider these key tips:

1. Start with Visibility

Identify all the accounts, privileges, and access points across your environment. Leverage tools that can provide you with unified visibility into your cloud and on-premise systems so you can map out your comprehensive identity security posture.

2. Adopt a Zero Trust Mindset

Implement least-privilege access policies for all identities, ensuring that users and services have only the

permissions they need, and continuously evaluate and enforce these policies as your environment evolves.

3. Leverage Automation

Replace manual processes with automated tools for threat detection, risk scoring, and remediation.

4. Integrate Real-Time Monitoring

Invest in solutions that offer continuous monitoring and real-time insights. Focus on platforms that can detect anomalies, identify misconfigurations, and provide actionable recommendations.

5. Secure Your Hybrid Environment

Address the unique challenges of bridging on-premise systems, like Active Directory, with cloud-native platforms, like Kubernetes and Entra ID.

6. Educate Your Teams

Equip your IT and security teams with training on modern security principles and the tools they'll use to implement them, and foster a culture of proactive security awareness across your entire organization—not just your security team—to ensure the smooth adoption of real-time security practices.

7. Plan for Scalability

Ensure your security solutions and processes can scale with your organization's growth and adapt to new technologies or threats.

In today's complex cybersecurity landscape, where attackers are much more likely to log in than hack in, having a real-time, adaptive approach to cybersecurity is not just beneficial—it's essential. By leveraging advanced cybersecurity disciplines that leverage emerging technologies, you can build a more resilient defense that will keep your organization one step ahead of evolving threats. ☺

Paul Da Silva is a Sr Solutions Architect at BeyondTrust, with over 15 years of experience. Paul's expertise covers a wide range of skills including Cyber Security Identity and Access Management (IAM), security architecture, incident response, all things Kubernetes & container and extreme curiosity in how everything works.



Strengthening Cybersecurity in Canada's Public Sector: Key Insights and Strategic Recommendations

by [Deryck Greer](#)

In today's interconnected world, cybersecurity is a critical national security priority. As digital transformation accelerates, countries face escalating threats from both nation-state actors and organized cybercriminal groups. Nation-states often engage in cyber espionage to gain economic or political advantage, while sophisticated criminal networks exploit vulnerabilities to disrupt services, steal data, and hold critical infrastructure hostage for ransom. The impact of these cyber threats can be severe, with repercussions not only for economic stability but also for public safety and trust. Strengthening cybersecurity resilience at the national level is essential for safeguarding Canada's infrastructure, maintaining the integrity of its institutions, and protecting citizens from the fallout of cyberattacks. These challenges require a cohesive approach across federal, provincial, and municipal levels, drawing on lessons from partners across the globe and the United States.

Overview of Canada's Cybersecurity Framework

At the federal level, the Canadian Centre for Cyber Security (CCCS) within the Communications Security Establishment (CSE) leads the country's cybersecurity initiatives, managing strategic guidance and coordinating responses to incidents. However, challenges remain, such as gaps in inter-agency collaboration as highlighted in the [Auditor General's Report on Cybercrime](#). The [National Cyber Threat Assessment 2025–2026](#) also underscores the growing risks from state-sponsored actors targeting Canada's critical infrastructure, governmental operations, and innovative sectors. To complement CCCS, the [National Cybercrime Coordination Centre \(NC3\)](#) was launched in 2020 by the RCMP as part of Canada's National Cyber Security and Cybercrime Strategy. The NC3 collaborates with law enforcement agencies, local governments, and private sector partners to address

cybercrime more effectively. It also works closely with the Canadian Anti-Fraud Centre (CAFC) on public cybercrime reporting and awareness.

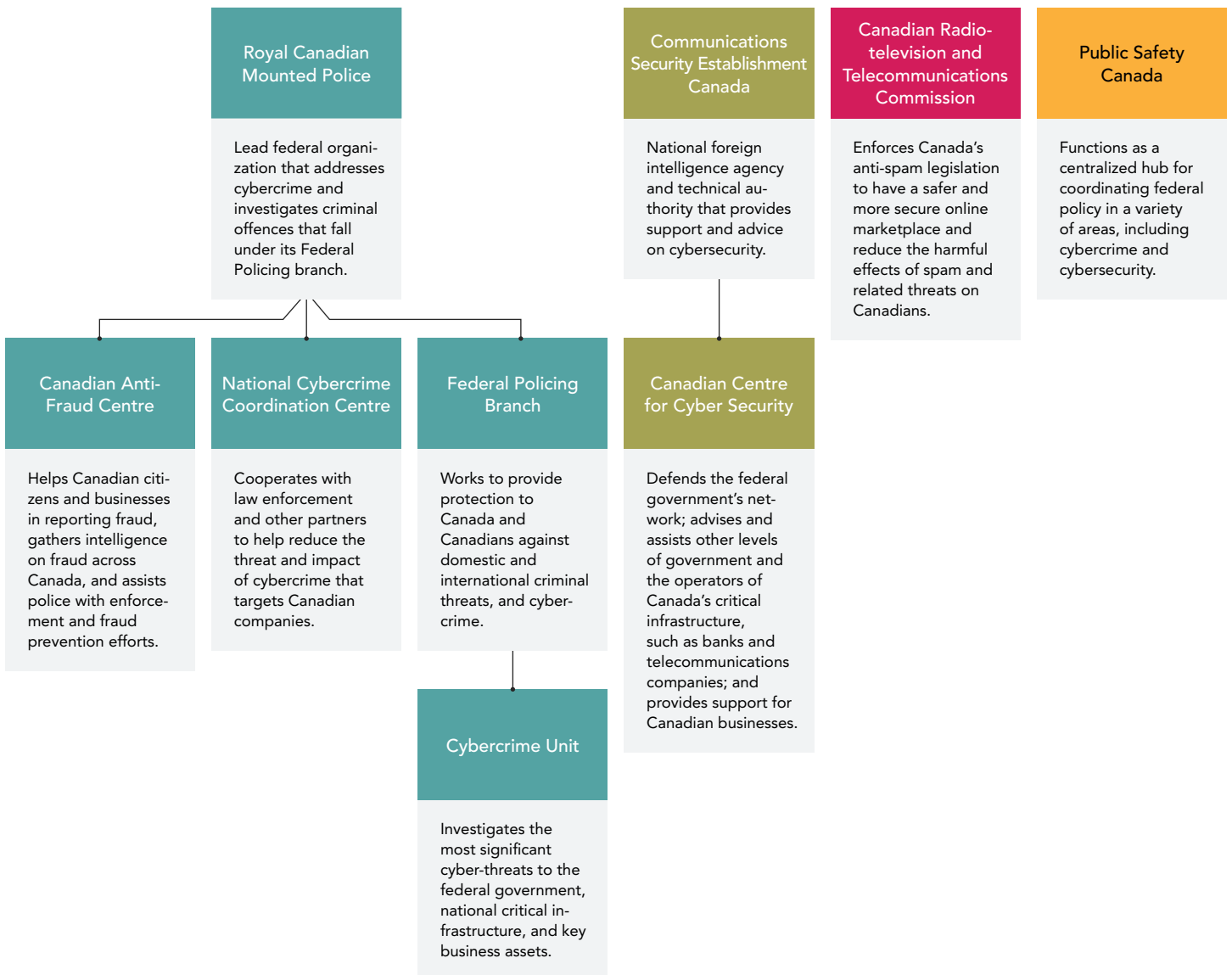
At the provincial level, each province is responsible for securing critical infrastructure sectors within its jurisdiction, such as healthcare, energy, and transportation. However, there are notable disparities in resources and capabilities across provinces, with smaller regions often facing more significant limitations. For instance, the 2023 ransomware attack on Alberta Health Services underscored vulnerabilities in the healthcare sector, which is a frequent ransomware target according to the [Canadian National Cyber](#)

[Threat Assessment 2025-2026](#). Provincial governments collaborate with federal bodies, but there is a need for more standardized approaches and additional support for provinces with fewer resources to ensure consistent cybersecurity measures nationwide.

At the municipal level, cities manage essential local services such as water, emergency systems, and transportation, but municipalities often have constrained budgets and limited access to advanced cybersecurity tools. The 2022 ransomware attack on Saint John, New Brunswick, exemplifies these risks, revealing the vulnerabilities faced by smaller municipalities. As noted in the 2021 report [An Industry](#)

Canadian Federal organizations with Cybercrime responsibilities

Source: Auditor Generals Report Combatting Cybercrime



Under Attack: Protecting the Oil & Gas Sector it stated that interconnected operational technology (OT) systems in industries like oil and gas increase cyber risks for cities dependent on these sectors. Municipalities can benefit from greater funding and support to implement cybersecurity programs, which would enhance local resilience and provide a more uniform defense across Canada.

Cybersecurity Structure in the United States: Comparing our closest ally

The United States takes a coordinated approach to cybersecurity across federal, state, and local levels, with significant resources allocated to federal agencies that support broader cybersecurity efforts. [The Cybersecurity and Infrastructure Security Agency \(CISA\)](#) plays a central role at the national level. Established within the Department of Homeland Security (DHS), CISA provides guidance, resources, and response capabilities to protect critical infrastructure across the country. Following high-profile incidents like the SolarWinds attack, CISA has received increased funding and expanded its mission to include enhanced inter-agency coordination and public-private collaboration, emphasizing the importance of resilience in critical sectors.

In addition to CISA's role, the United States has implemented federal programs like the [State and Local Cybersecurity Grant Program](#) to support state and municipal efforts to strengthen cybersecurity defenses. The program provides grants to state governments, which can allocate these resources to local governments to improve cybersecurity training, secure critical infrastructure, and enhance threat detection capabilities. Additionally, National Guard cyber units can assist in emergency situations, providing technical expertise and rapid response to cyber incidents at the state level.

CISA also plays a critical role in establishing security standards and sharing actionable threat intelligence across all levels of government and private sector partners. To support these efforts, CISA provides technical remediation recommendations and even offers free cybersecurity tools, which help organizations improve their defenses without additional budgetary strain. These resources include scanning and testing services, guidance on security practices, and technical support aimed at preventing and mitigating cyber threats. Together, these initiatives foster a cohesive cybersecurity structure that bridges national resources with local needs, ensuring a robust, layered defense across the U.S.

Vulnerabilities and Emerging Threats Across Key Sectors

OIL AND GAS

The oil and gas industry's reliance on interconnected IT and OT systems makes it particularly vulnerable. According to the world economic report cyber adversaries target this sector for economic espionage, aiming to steal intellectual property and disrupt production. A 2023 ransomware attack on [Suncor Energy](#) underscores the substantial financial and operational impacts these attacks can have. Key challenges in this sector include legacy OT systems, secure remote monitoring, and the high value of intellectual property.

HEALTHCARE

Healthcare is highly vulnerable to ransomware due to the sensitive nature of patient data. In 2023, [Alberta Health Services](#) suffered a ransomware attack that disrupted patient care, and healthcare accounted for over 25% of ransomware incidents reported in Canada in 2022, as noted by the NCTA. Outdated infrastructure, extensive data-sharing needs, and the sensitivity of patient records present unique cybersecurity challenges in this sector.

Emerging Threats

Both the NCTA and Combatting Cybercrime report emphasize several emerging threats:

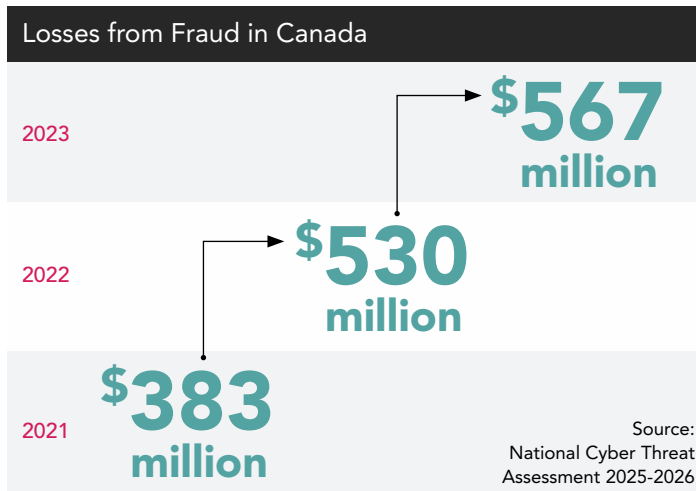
- 1. AI-Powered Phishing:** AI-generated phishing messages are increasingly sophisticated and harder to detect.
- 2. AI-Exposed Software Vulnerabilities:** AI is now being used by hackers to identify coding errors in software that could be exploited by malware toolkits.
- 3. Supply Chain Attacks:** Targeting third-party vendors is a growing risk, with cybercriminals exploiting access points to compromise entire supply chains. Increasingly, hackers are injecting malware directly into third-party software products that are consumed downstream by customers, creating widespread vulnerability. A prominent example of this type of attack is the SolarWinds breach in 2020, where attackers injected malware into the company's Orion software update, affecting thousands of customers, including U.S. federal agencies and large corporations. This breach underscored the risks of supply chain vulnerabilities, as malicious code embedded in trusted software updates can infiltrate numerous organizations simultaneously.

4. Advanced Ransomware Tactics: Attackers are increasingly using “double extortion” strategies, where data is both encrypted and stolen to demand higher ransoms.

The WEF’s “Unpacking Cyber Resilience” report further highlights the need for resilience in sectors like energy and healthcare, stressing preparedness and system redundancy to maintain operational integrity under attack.

Economic Impact and Strategic Recommendations

Cyber incidents are estimated to cost the Canadian economy over CAD 5 billion annually, with operational disruptions, recovery expenses, and reputational damage affecting multiple sectors. Ransomware attacks, in particular, impose significant financial burdens on industries such as healthcare and energy. Meanwhile, challenges in prosecuting cybercrime persist, as highlighted by the Auditor General’s Report on Cybercrime, which notes limited law enforcement resources and the resulting difficulty in bringing cybercriminals to justice. To strengthen Canada’s cybersecurity posture, expanded federal resources and coordination would enhance the CCCS’s capacity to manage complex cyber threats. Establishing a centralized body, similar to the U.S. Joint Cyber Defense Collaborative (JCDC), could further improve inter-agency alignment.



For provincial resilience, a standardized cybersecurity framework with federal support could provide provinces with consistent protections across critical sectors. This model, resembling U.S. state-level support structures, would ensure that smaller provinces have access to essential resources for defense. Similarly, a dedicated funding program for municipalities could equip local governments to build cybersecurity teams, improve threat monitoring, and modernize critical infrastructure. Canada should also

focus on enhancing public-private partnerships to support collaboration on threat intelligence, following models like the U.S. JCDC to boost defenses in key industries, including oil and gas.

Sector-specific resilience strategies would also be valuable. For example, in the oil and gas sector, adopting Zero Trust Architecture and securing IT/OT integration would address unique vulnerabilities. In healthcare, upgrading outdated systems, conducting regular cybersecurity training, and strengthening data encryption protocols would bolster defenses. Additionally, enhancing supply chain security through robust vendor assessment protocols would mitigate risks across critical sectors.

As an example, The National Council of Information Sharing and Analysis Centers (ISACs) in the United States of America consists of 27 member organizations, each dedicated to enhancing cybersecurity resilience within specific sectors by facilitating information sharing and threat intelligence among companies in their respective industries. These ISACs cover a wide range of sectors, including energy, healthcare, financial services, and transportation, enabling industry-specific collaboration to address common threats and vulnerabilities. By providing timely, relevant intelligence, ISACs play a critical role in strengthening sector-specific defenses and improving coordinated responses. Establishing similar sector-focused information-sharing hubs in Canada would reinforce cross-industry defenses and improve coordinated responses to sector-specific threats.

Conclusion

Canada faces significant cybersecurity challenges, with critical sectors increasingly susceptible to complex cyberattacks. The National Cyber Threat Assessment 2025–2026 emphasizes the importance of a proactive, coordinated approach. Embracing strategies that draw on successful U.S. models, along with increased federal support and enhanced sector-specific defenses, will be essential for Canada to fortify its digital resilience and protect its essential infrastructure against evolving cyber threats. ⁸

Deryck Greer is the Chief Information Security Officer for Protexxa. He is a former security cleared senior cybersecurity and intelligence leader with over 18 years of professional practice across multiple domains including but not limited to; cyber intelligence, cyber operations, and law enforcement.



Cyber risk can't be solved with technology alone

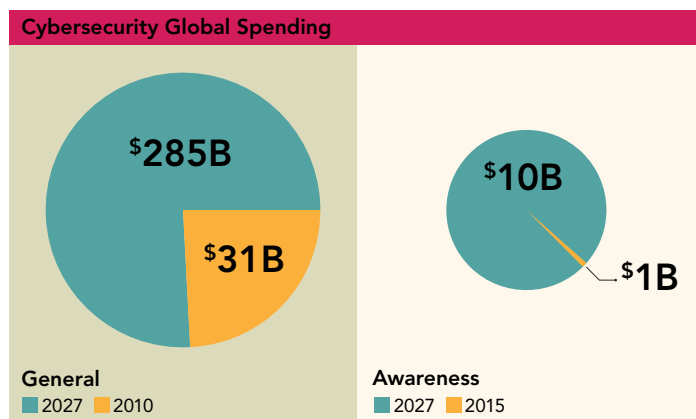
by [David Shipley](#)

For more than 50 years, since the advent of the first anti-virus tool Reaper,¹ the world has been more focused on using technology tools to combat digital threats than it has been in dealing with the human aspects of cybersecurity, by a significant margin.

In the last 15 years, spending on cybersecurity globally has surged from \$31 billion in 2010² to an estimated \$285 billion by 2027³, an 819% increase in spending, yet paradoxically the threat environment has failed to improve in any appreciable way. Over the past decade, cybersecurity awareness spending is estimated to have grown from \$1 billion in 2015⁴ to as much as \$10 billion by 2027⁵. In

terms of per cyber dollar spending, cybersecurity awareness has gone from 1.4 cents per cyber dollar spent to 3.5 cents per cyber dollar by 2027⁶, a 150% increase but still only a tiny part of the overall spend.

While admittedly part of the reason for the escalating losses despite the surge of investment is an ever-increasingly hostile online environment driven by major geopolitical, technological and criminal shifts over the past 30-years, arguably the fact that we keep focusing mostly on technological solutions to the problem (and getting the same abysmal results) instead of increasing the money and time investment on the human side of cybersecurity is part of the overall story.



The clues hidden in the word cyber

The word cyber comes from the Greek word, kybernetes.⁷ Norbert Wiener, father of the field of cybernetics and an MIT mathematician and philosopher, borrowed this Greek word with deliberate intention. Wiener wanted to find a way to encapsulate the three critical elements and the relationship between those elements that his new science would study.

Kybernetes, which means the helmsman or steersman on a ship, perfectly captures this concept. If you picture in your

mind's eye an ancient Greek ship, at the back of this ship is the first element of cyber: the human. In their hand is the oar, the rudder, the ship's steering wheel, which represents technology: the second element. The third and final element in this image is control.

Humans in control of the technology they create is the story of progress, from the earliest and most powerful transformational technology we ever invented, fire, to the modern digital economic nervous system that is the Internet today.

The story of technology in control of humans rarely ends well, whether it's Skynet and Terminators in the famous movie franchise, or Tesla "full self-driving" cars that keep killing people on highways, or the Boeing Max 8 disasters where flawed sensors and software killed hundreds by taking control from the jets' pilots; the evidence is clear. We can't technology ourselves out of cyber risk.

Humans in control of the technology they create is the story of progress, from the earliest and most powerful transformational technology we ever invented, fire, to the modern digital economic nervous system that is the Internet today.

Even the current zeal around technology security focused concepts like zero trust⁸ ignores the reality that the tools we depend on to enforce that concept and ensure security themselves contain flaws as the products of humans.

Take the example of a flaw in one of the world's most popular e-mail filters that allowed millions of phishing e-mails to impersonate well-known brands⁹ or the flaws in popular firewalls¹⁰ that allowed them to be used against defending organizations¹¹. Then there's also the human error that can come from how client organizations implement security tools, such as cloud-based e-mail filters. In one academic study, it was estimated that 80% of .com and .edu domains using cloud-based e-mail filters had misconfigured them in a way that attackers could use to deliver phishing attacks¹².

Often firms make bold claims about the efficacy of technology controls. Take e-mail filters, many of which claim to have phish catch rates as high as 99.98%¹³, but in fact can have false negative or phish leakage rates as high as 30%. In Beauceron Security's real-world testing over more than six months, Microsoft's Advanced Threat Protection had an 8.5% to 9% leakage range.

The leakage range comes from a review of at all the e-mails Microsoft said it stopped, including false positives, and then added all the real phishing e-mails that had been delivered to employee's inboxes that were then spotted and reported by employees. We then used the employee reporting rate percentage from phishing simulations to calculate how many real phishes may have been delivered but not reported.

The reality of technology is that if it is built by humans, it will always be as beautifully flawed as its creators and there will always be creative human minds that will find ways to defeat it.

This isn't to say that organizations should abandon technology security controls or that technology security controls built with a defense-in-depth approach do not provide clear, demonstratable value.

A well-educated and well-motivated team combined with a robust, positive security culture is the equivalent of a well-trained defensive driver in a modern car in busy traffic. The addition of technology controls in the car such as blind spot assistance, adaptive cruise control and forward collision alerts augment the drivers' skill and enable the greatest possible safety.

The essential components of human-centric cybersecurity

There are four critical elements to human-centric cybersecurity: people, process, culture and technology. These four aspects are critical to developing comprehensive approaches that can enable organizations to reduce cyber risk and thrive in a digital environment.



1. PEOPLE

First and foremost, do the people in an organization have the knowledge and the motivation to apply that knowledge in their specific roles? This requires going beyond tired

approaches of simply mandating people to take computer-based training as part of compliance regimes. It requires going from security awareness training (SAT) to security behavior and culture programs (SBCP) an approach that merits further exploration on its own.



2. PROCESS

It's one thing to ensure education is available and that people are motivated about security; it's another to ensure that processes are in place to support and reinforce that work. A glaring example in most organizations is the lack of follow-up to end users who report suspicious e-mails as they have been educated to do through security awareness and engagement programs. Less than 10 percent of organizations in our experience are doing this work, though those who do it see as much as a 50% higher report rate.

Organizations that have tools to help automate the response to reported suspicious e-mails can scale this work and tailor the responses with just-in-time learning about the reported e-mail. In our experience, as many as one in four reported e-mails can be legitimate business that requires employee follow-up and attention. Closing the feedback loop not only encourages reporting, but it also reduces unintentional negative productivity impacts of suspicious e-mail reporting.

Process goes beyond this specific example and includes everything from ensuring people know the *who* and the *how* of getting help with a security concern or question. It also involves ensuring leadership knows how their incident response plan and processes work through regular practice via tabletop exercises.



3. CULTURE

In a Forrester study in security culture, which included responses from 1,161 people, 758 unique definitions were given for security culture¹⁴. A third of respondents said security culture was compliance with security policy. A quarter of respondents said it had to do with awareness and understanding of security issues. A fifth of respondents said it was the recognition that security was a shared responsibility throughout the organization.

In our work, Beauceron has proposed a new definition of security culture. Our definition of security culture is the norms and values in an organization, expressed and implied, in how individuals and leadership make decisions about their use of technology.

We help measure this through metrics around individuals' knowledge, perception, motivation and the organization's process and technology related to cybersecurity. Organizations with a positive security culture not only benefit from reduced risk, but they also make good decisions about when, where and how to use technology to further their goals.



4. TECHNOLOGY

As noted earlier, technology controls to mitigate cyber risk remain essential within a human-centric cybersecurity strategy. Relying on people alone would be ruinous for organizational productivity. This would be the equivalent of building a modern car and expecting it to be propelled by the occupants with their feet, like the cars in the Flintstones.



Technology goes beyond mitigating controls for cyber risk such as e-mail filters, firewalls and endpoint detection and response. It also involves the design of the software and tools people use every day. For example, one of the greatest security innovations Microsoft Outlook could include would be a warning when someone has been reading and replying to e-mails for too long, encouraging them to take a break. Think the coffee icon that modern cars can display if drivers are detected to be weaving in a lane potentially due to exhaustion.

It is worth noting that there's a special caution about the intersection of technology controls for cyber risk and the perceptions team members have about the effectiveness of those controls. In our research, employees who believe security technologies such as e-mail filters, firewalls and endpoint detection completely protect them from Internet threats have average phishing e-mail click rates that are up to 97% higher than those who don't believe such tools provide complete protection.

The key to unlocking the potential of people, to help them understand your processes and to leverage them to the best advantage, to creating and sustaining a positive security culture and to enabling good choices about technology, is robust security engagement, education and motivation (SBCP) program.

From Security Awareness Training (SAT) towards Security Behaviour and Culture Programs (SBCP)

The need for information security awareness and the potential to build platforms and use computer-based training goes back more than 30 years¹⁵. It's worth noting that 30 years ago a key issue was identified that has been lost over the years; the idea

that security awareness had to be about more than knowledge dissemination. It must be about approaches and content that motivates people to care about cybersecurity. Even in the context of the US defense sector in the cold war, motivation was noted as a persistent challenge:

“For the vast majority of personnel, security concerns are a low priority... Even during the times that they are engaged in security-related tasks, their motivation to succeed in these tasks will be low. Security education must either find ways of raising motivation or of ensuring that security is protected even when motivation is low...”¹⁶

What's fascinating about the Security Awareness in the 90s symposium paper published by the US Department of Defense in December 1990 is how applicable it remains today and how far ahead of its time it was in the context of the modern challenges of information security, not only for the defense sector, but now the entire economy.

“Part of the motivation problem is the lack of natural rewards. Security measures, by their nature, are successful only when nothing happens. Feedback on security related tasks is almost always negative. Because rewards are far more effective training devices than punishments, security educators must find ways of introducing positive feedback into their efforts or ways of living with the reduced training effectiveness provided by negative reinforcement.”¹⁷

Somehow, over the past 30 years, as security awareness evolved beyond the defense sector and was adopted throughout every industry as they embraced digital technologies and the Internet to fulfill their missions, the importance of motivation was lost.

The loss of focus on motivation is likely tied to the initial evolution of security awareness as a largely unwelcomed add-on to already overworked information technology teams. As chief information security officers became a key part of the leadership of organizations, as threat actors use of social engineering (the expert use of emotional manipulation via e-mail, known as phishing) exploded, security training was seen as a way of dealing with the “people problem” and or as mostly a compliance check-the-box activity.

People become more likely to click on phishing e-mails when they think either their organization is not a target, or they aren't personally a target for cybercrime.

The stupid people fallacy

The “people problem,” also known as the “humans as the weak link or stupid user problem” in security, remains deeply flawed. First, it presumes that technology is not flawed itself, which as noted earlier with examples of zero-day exploits for firewalls, e-mail filters and more, is clearly not the case. There is however a deeper argument against the “human as the weakest link” fallacy. If an organization was truly filled with stupid people, cybersecurity is not the biggest risk. The fact it's filled with stupid people would be the biggest risk.

Most organizations are not full of stupid people. Most team members in an organization not only want to do the right thing, but they are also the organizations most valuable competitive asset. Beauceron's research has consistently found 90%+ of organizational members care about the important role they play in cybersecurity.

The challenge for security educators is ensuring people know why and how to apply security knowledge provided.

The top 10% of organizations have median phishing simulation report rates of 56%, which is more than double the overall median report rate across our entire customer base.

The components of an effective SBCP program

There are three key parts of an effective security behaviour and culture program. These components are tied to previous neuroscience work in the workplace, notably Dr. David Rock's SCARF model. The three components of a modern SBCP program are: evaluate, motivate, and educate.

1. EVALUATION

For measurement, organizations must first establish a qualitative baseline of employees' knowledge and attitudes. Often such measures, conducted with surveys, are dismissed by technology centric cybersecurity professionals in favour of qualitative data from systems. However, that ignores that the only way to ascertain what someone knows and believe is to ask them about it and to listen to what they tell you. Surveys can yield tremendous insights, as our research has shown. Answers to these surveys can be compared to qualitative security performance data (for example, phishing simulation click and report rates), to understand the potential risks of some beliefs or attitudes. One such example mentioned earlier is the framing bias that people may have around the efficacy of technology controls. People who see technology controls as 100% protection become much more prone to click on phishing e-mails, with the median click rate for that group being 7%, compared the median click rate for those who strongly disagreed, which was 3%.

Another bias we've seen from this data includes optimism bias, which is the natural tendency for humans to think that bad things are more likely to happen to someone else rather than to themselves. People become more likely to click on phishing e-mails when they think either their organization is not a target, or they aren't personally a target for cybercrime.

Conversely, people who do believe they play an important role in protecting their organizations or that cybersecurity is everyone's business are much more likely report suspect phishing e-mails.

2. MOTIVATION

As humans, we're incredibly sensitive to elevation or loss of status and are intrinsically motivated to pay attention to such changes. While employees can be motivated through quiz scores or thank you messages after they report

phishing simulations, providing more feedback creates a powerful motivator. Our work has shown that systems such as competitions or an easy-to-understand cyber risk score can influence learning and behaviour. This effect, which we often compare to what the Apple Watch or Fitbit did for exercise, allows us to tap in the status portion of Dr. Rock's SCARF model¹⁸.

A key component of this motivational approach is reinforcement. As noted in the 1990s work, negative reinforcement is a valuable tool, but it can only go so far. Organizations that do better at recognizing when people do the right thing – from reporting phishing e-mails to sharing security concerns to using security tools like password managers well – will do better at creating motivational impact and positive security cultures. A personal cyber risk score metric creates the mechanism to support positive and negative reinforcement.

3. EDUCATION

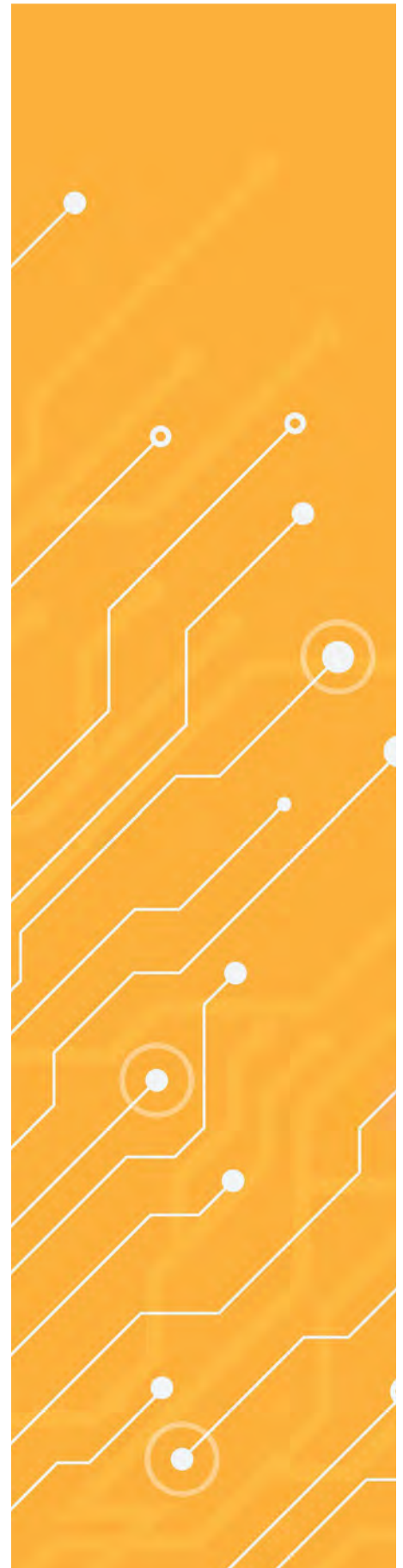
When it comes to education, much more attention must be spent in SBCP programs compared to old-school SAT approaches about the amount of education provided at time, the key messaging, and frequency of education, as well as the delivery mechanism. Recent studies claiming that anti-phishing simulations don't work were based on the failure of one educational delivery mechanism: post-click webpages that load static or interactive content. Those outdated methods do not engage people, with the vast majority staying on page less than 30 seconds (and in some cases, less than 10 seconds). On the other hand, educational modules focused on emotional intelligence and assigned through a learning portal were much more likely to be engaged with and much more likely to be successful.

Testing the effectiveness of knowledge dissemination is critical. Anti-phishing education done with effective, fair and rewarding phishing simulations are a continued critical component of an SBCP program. Our work has shown that organizations that do monthly, adaptive difficulty phishing simulations on a per employee basis see the best risk reduction in terms of lowest median click rates and the best results in report rates. While click rates can and do fluctuate based on lure difficulty and will always contain an element of chance in that people accidentally click, report rates remain a much more valuable indicator of knowledge and attitude as people must recognize something is wrong with the e-mail and are motivated to report it.

This sequence of evaluate, motivate and educate is a continuous cycle and it leads to measurable individual cyber risk performance improvement as well as positive security culture development and reinforcement.

The work on the human side of cyber is not easy, quick, or something that can be solved with a technology platform alone. Yet it offers the single largest opportunity for further risk reduction with the best possible return on investment if done through a modern, SBCP approach. 🧠

David Shipley is the CEO and Co-Founder of Beauceron Security Inc., a New Brunswick-based cybersecurity software firm with clients across North America. David is a certified information security manager and frequently writes and speaks about cybersecurity issues across North America.





Building Digital Trust: A Strategic Imperative

Digital trust involves respecting privacy, safeguarding data, managing cybersecurity threats, ensuring transparency in data usage, and embedding trust in an organization's strategy and culture. There is a critical link between digital trust, sustainable growth, competitiveness, and business success.

AI's impact on digital trust is significant; hence, mitigating the potential risks associated with the technology is essential. Trust in AI cannot be assured by technical means alone and must involve the development of ethical and transparent AI governance structures.

Key standards fostering digital trust and operational resilience include:

- ISO/IEC 27001:2022, Information security management (cybersecurity)
- ISO/IEC 27701, Security techniques (data governance and protection)
- ISO/IEC 20000-1:2018, Service management (digital services)
- ISO/IEC 42001:2023, AI Management system
- ISO 22301:2019, Business continuity management

Certification to ISO standards offers numerous benefits to organizations across various industries.

Whatever the size of your business, BSI can help establish, implement, maintain, and continually improve your information security and business management systems to help you strengthen your operational resilience.



Your partner in progress

1-800-862-6752
inquiry.mscanada@bsigroup.com



Securing excellence: A guide to an information security management system

by [Caio Cogni](#), Presented by BSI Group

Building cyber

Data and connectivity are accelerating the extraordinary transformation of organizations, from establishing digital ecosystems to optimizing supply chains and operational procedures. However, as technology progresses, the certainty of cyberattacks, data breaches, and other operational disruptions grows.

The ability to manage information safely and securely has never been more critical. Organizations must build resilience around their information security management systems (ISMS) with an internationally recognized framework like ISO/IEC 27001. This standard helps organizations prioritize safety, privacy, reliability, cybersecurity, and data ethics throughout their organization while maintaining an ISMS aligned with global best practices.

The average cost of a cyber breach in 2024 was USD \$4.88 million.

The costs and disruptions caused by information security breaches are rising, leading to substantial damage to organizations.

An ISMS can help protect organizations and reduce risk by applying a robust and systematic approach to managing information. This standard can aid in defending an organization's reputation, saving money, achieving compliance, and reducing risks. Maintaining a secure environment requires implementing industry standards, demonstrating proper procedures, and promoting confidence in clients, employees, and stakeholders through robust information security practices.

There are 63 published standards under the ISO/IEC 27000 family. They provide information security best practice recommendations covering privacy, confidentiality, and cybersecurity issues. Here are the most prevalent standards organizations adhere to:

- **ISO/IEC 27001:2022**
- **ISO/IEC 27017:2015**
- **ISO/IEC 27018:2019**
- **ISO/IEC 27701:2019**

Benefits

Inspires digital trust in your business

Provides greater reassurance to your clients and stakeholders that data and information are protected.

Competitive advantage

Demonstrates robust controls are in place to protect data.

Protects your brand

Reduces the risk of adverse publicity due to data breaches.

Helps reduce risks

Adherence to the standard aids in identifying risks by requiring the implementation of controls to manage or reduce them.

Supports compliance

Supports compliance with local regulations, reducing the risk of fines for data breaches.

Fortifies business growth

Provides common guidelines across different countries, making it easier to do business globally and gain access as a preferred supplier.

Top tips on making an ISMS impactful

Top management commitment is key to implementing ISO/IEC 27001 successfully.

“The earlier that organizations talk to senior managers, the better it will go for them, so have those discussions early.”

—John Scott, Manager, Overbury, leading UK fit-out and refurbishment business

It's important to make sure an organization works as a team for the benefit of clients and the organization, avoiding silos.

“The key to implementing the standard lay in getting staff to think about information security as an integral part of the daily business and not as an additional burden.”

—Mr. Thamer, Ibrahim Ali Arab, Assistant General Manager, I.T.

Review systems, policies, procedures, and processes in place – it needs to add value.

“Don't try and change your business to fit the standard. Think about how you do things and how that standard reflects on how you do it, rather than the other way around.”

—Paul Brazier, Commercial Director, Overbury

Speak to clients and suppliers. They may be able to suggest improvements and give feedback.

“This certification allows us to go one step further by offering our customers the peace of mind that we have the best controls in place to identify and reduce any risks to confidential information.”

—Jitesh Bavisi, Director of Compliance, Exponential-eBavisi

Training staff to conduct internal audits of the system can help them better understand the requirements and provide valuable feedback on potential problems or opportunities for achievement.

“The course was loaded with practical exercises and real-case scenarios and was structured in a way that it encouraged participants to be interactive and share their experiences in information security.”

—Nataliya Stephenson Manager, Information Security, NSW Attorney General's Department

Certification to an ISMS

Obtaining ISO/IEC 27001 is a critical initiative that supports your company's ongoing success and resilience in today's ever-changing business landscape. Adhering to the meticulous standards set forth by an internationally recognized framework helps to fortify information security practices and demonstrate a steadfast commitment to protecting your assets, maintaining client trust, and supporting regulatory compliance.

Through regular risk assessments, audits, and reviews, you can refine your security protocols, adapt to evolving threats, and stay ahead of emerging challenges.

This standard fosters a culture of continuous improvement. Through regular risk assessments, audits, and reviews, you can refine your security protocols, adapt to evolving threats, and stay ahead of emerging challenges. This process enhances your security posture and promotes operational efficiency and resilience across the business.

Additionally, your certification serves as a powerful distinguisher in the marketplace. It provides tangible evidence to clients, partners, and stakeholders that you take information security seriously and adhere to globally recognized best practices. This can open doors to new business opportunities, bolster client trust, and give a competitive edge in industries where security and confidentiality are vital.

Adopting ISO 27001 is not just a strategic move; it's a proactive investment in your company's future. By prioritizing information security, you can enhance your reputation, safeguard assets, promote innovation, and drive sustainable growth in an increasingly interconnected and digitized world. ⁸

Caio Cologni, Business Development Manager, BSI Canada, is a recognized expert in information security, cybersecurity, and privacy frameworks, with over a decade of experience helping organizations with internationally acclaimed standards like ISO/IEC 27001. As business development manager at BSI Group Canada, Caio works closely with organizations across industries to enhance organizational resilience against cyber threats through certifications, training, and strategic guidance.

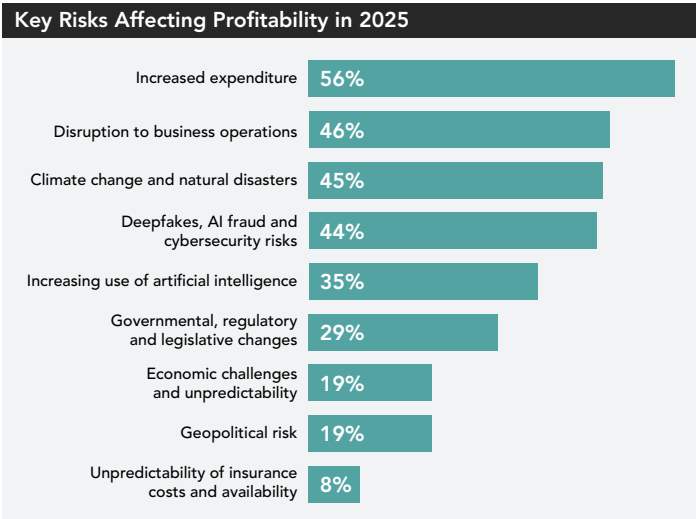
His deep and comprehensive knowledge of the ISO/IEC 27000 family of standards enables him to provide actionable insights on building a robust Information ISMS. His expertise, honed over years of dedicated work, has empowered countless businesses to safeguard data, build trust, and achieve compliance in a rapidly evolving digital landscape.





The Cyber Insurance Market By Jonathan Weekes

Discussions around cyber over the past few years have shifted toward three areas: effective risk management, the pursuit of resiliency and the need to view cyber as an organizational risk rather than a technology risk. The insurance industry has played a key role in not only driving an understanding of cyber risks across organizations in all industries but also providing practical solutions for companies to assess, quantify and manage cyber risk, including the use of risk transfer solutions such as insurance.



Both New and Familiar Risks Threaten Company Profits

Survey results from [The Hub International 2025 Outlook North American Report](#) reveals that the key risks to profitability in 2025 continue to include cybersecurity risks, including deepfakes & AI fraud. While respondents report a high level of preparedness to managing the impact of increased expenditures and business disruption on profitability, they concede that they are less prepared to handle climate change and cyber risks.

Canadian survey respondents expressed greater confidence in their preparedness to tackle key risks to profitability compared to their U.S. counterparts but rated themselves as less prepared to respond to climate change, AI adoption and regulatory changes. Of the executives surveyed, only 44% stated that they are prepared to address cybersecurity risks and only 53% felt that they were prepared to tackle risk challenges tied to the increased use of artificial intelligence.

Is Cyber Insurance Still Worth Exploring?

For years, cyber insurance has been an effective means for organizations to transfer residual risk associated with privacy and information security exposures. Cyber insurance

as a product has existed in one form or another since 1997, when it was first offered by American International Group (AIG), a US-based insurance company. Throughout the years, these policies have evolved from offering coverage focused primarily on liability arising out of privacy breaches, to comprehensive policies covering losses stemming from everything from ransomware and data destruction to non-malicious system outages.



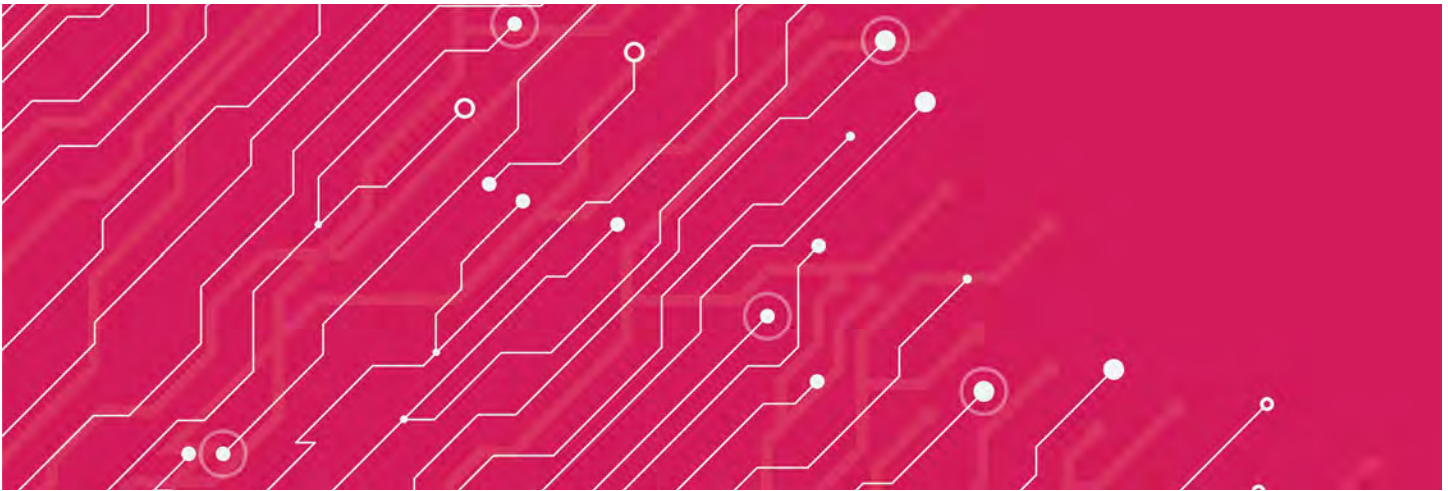
Any organization that has purchased cyber insurance for an extended period would have seen drastic changes to the cyber insurance market over the past 5 years. The proliferation of ransomware starting in 2018, amplified by the rapid expansion of remote work triggered by the global COVID-19 pandemic, drove the cyber insurance industry into a hard market. A “hard” insurance market refers to a period during which the availability of insurance capacity is limited, and rates increase drastically, typically due to higher-than-expected losses in any given underwriting year.

While cyber insurance has proven more onerous and costly for larger organizations to purchase over the past 3 to 4 years, many buyers will agree that it not only forms a critical part of their overall risk management strategy, but also that the cyber insurance market has shown significant signs of improvement over the past several quarters. Despite the cyber insurance market softening over recent years, the HUB survey indicates no discernable increase in cyber insurance buyers year over year, with only 40% of respondents reporting that they have some form of cyber coverage.

What does Cyber Insurance Coverage look like today?

With the average cost of a data breach in Canada sitting at USD 4.66M, according to the IBM Cost of a Data Breach Report 2024, cyber insurance remains one of the most effective ways for organizations to transfer financial risk tied to cyber events. Cyber insurance policies continue to cover a broad range of risks through the provision of coverage including:

- **Cyber Event Management** coverage, which reimburses the policyholder for out-of-pocket expenses incurred to engage legal support, computer forensics, public relations & more, in the handling of a privacy or security breach. This part of the policy also reimburses clients for costs to notify and provide credit monitoring to impacted individuals, whose confidential information may have been impacted.
- **Digital Asset Restoration Costs** which, covers the costs to restore and/or repair lost or damaged data in the event of a network security failure and to determine what data cannot be restored, recollected, or recreated. This coverage is sometimes extended to include brick-ing, which will replace network equipment, should it be rendered inoperable as a direct result of the information security breach.
- **Cyber Extortion**, the area of coverage that has seen the highest severity of loss in recent years, reimburses the insured for reasonable and necessary expenses incurred in responding to a network extortion threat, generally tied to ransomware. This coverage includes negotiation costs and ransom payments to the party thought to be behind the threat, where permitted by law.
- **Business Interruption & Extra Expense** coverage reimburses policy holders for lost income and extra expense resulting from a network security breach that leads the actual and measurable interruption, suspension or impairment of an insured’s computer systems or business operations. Coverage is often also extended to loss of income resulting from impairment of a third party’s computer systems, SaaS, PaaS, IaaS on which the insured relies upon for regular operation of its business. The strongest policy wordings further expand coverage to include system failure as a trigger of coverage. While the standard business interruption coverage will only respond when the cause of loss is a malicious third-party attack, the system failure coverage goes further include loss of income resulting from any unplanned, unintentional, or unscheduled network outage. A good example of this is the widespread disruption tied to a CrowdStrike update in summer 2024.



- **Privacy & Security Liability** provides coverage for defence costs and damages arising out of the failure to protect sensitive personal or corporate information in any format, for which the insured is legally responsible. This section would also cover insureds for defence costs and damages arising out of the failure of network security, including unauthorized use of corporate systems, a denial-of-service attack, or the transmission of malicious code.
- **The Regulatory Proceedings** coverage in cyber policies responds to cover defence and investigation costs in the event of an investigation by a governmental or regulatory entity. Regulatory fines and penalties may be covered, but only where insurable by law. This is an aspect of coverage where we have recently seen more claims, with changes to privacy regulations in Canada and globally.

When purchasing cyber insurance, it is critical for organizations to possess an understanding of what is covered as well as the types of events that might not be covered. Most cyber policies exclude things like telecommunications and critical infrastructure failure, misconduct or criminal acts of senior executives and bodily injury and property damage. Cyber insurance buyers should dedicate as much time to reviewing the exclusions under the policy as they do the insuring agreements. A good broker will take the time to walk through the various elements of coverage, while comparing the offerings from various insurance companies to pick the option that best aligns with your needs.

How can an insurance broker can help?

- **Brokers can provide** insights into the health of your cyber security program through an objective, data-driven lens that identifies exposures and hidden risks

- **Use advanced cyber** benchmarking tools to help determine the appropriate limits relative to an organization's exposure
- **Evaluate your organization's** exposure by considering important factors such as how much customer data your organization retains, your record retention policies and frequency of cyber security training for employees

What is next for cyber insurance?

Much like cyber risks themselves, cyber insurance policies will continue to see shifts in coverage, minimum requirements to qualify and value-added services offered by insurers. The role of insurance brokers also continues to evolve, with many of them focusing more on risk management services and solutions in addition to their core function of placing insurance coverage on behalf of their clients.

In 2025, we will likely continue to see a further stabilization of the cyber insurance market, with rates flattening, coverage continuing to expand and more new buyers entering the market. Cyber insurance should be considered when developing or revising an organization's cyber risk management strategy, as it can help to address the residual financial risk that exists after implementing appropriate information security governance and controls. We will likely see continued pressure from boards and trading partners for organizations to procure or considering procuring the cyber insurance, so it is best to start the process sooner than later. ☺

Jonathan Weekes is HUB International Canada's cyber practice leader, Jonathan is responsible for developing client-specific product solutions, advising clients on issues related to cyber risk, negotiating with insurers, and educating clients and colleagues on emerging technologies.

Your data is everywhere. Your defences aren't.

Protect your hybrid environments and SaaS applications with GlassHouse Systems
24/7 Managed Security (MSSP)



ghsystems.com/resilient-enterprise



[Start with a no-cost data
resiliency assessment](#)

IBM
Platinum Partner



A Novel Approach to Data Protection

by Christopher Lee, Presented by [GlassHouse Systems](#)

Cybersecurity attacks are all about data: personal, corporate, healthcare, financial, or intellectual properties.

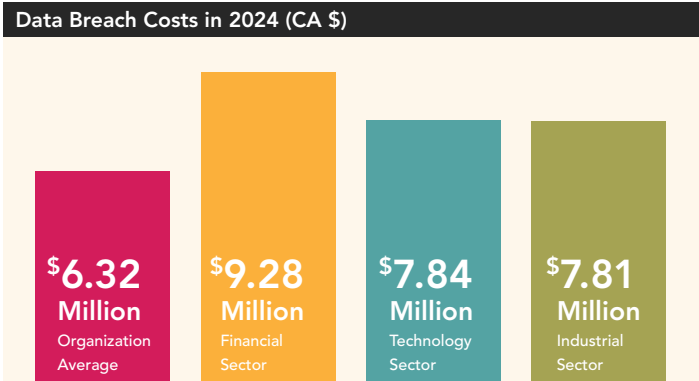
Data-motivated attacks are becoming more frequent, aggressive, and ultimately more costly. The attack style varies, but whether through ransomware, espionage, unauthorized disclosures, or destruction and denial of availability—cyber adversaries are fixated on acquiring your critical information, and they have a good reason.

Sensitive information, such as personally identifiable information (PII), credit card numbers, corporate financials, healthcare records, and intellectual property, is the organization’s bloodline and, in many cases, its secret sauce. Once seized by an attacker, these assets quickly become the organization’s largest threat.

According to the [IBM Cost of Data Breach report](#), in 2024, Canadian organizations paid an average cost of CA \$6.32 million per data breach. The financial sector paid \$9.28 million on average per breach, the technology sector is

paying \$7.84 million on average, and the industrial sector pays \$7.81 million on average.

Interestingly, in most of the cases, breached organizations have security, controls, and policies in place, yet their critical data ended up in the wrong hands and was used against them. The average financial damage caused by a single breach reaches startling heights, underscoring the reality that conventional approaches may be faltering.



Despite deploying robust edge and network security, threat intelligence tools, and security programs, organizations across industries remain vulnerable. The facts suggest that our traditional, and often dogmatic, defence strategies might be failing to offer real, long-term protection.

It's time to ask ourselves: are our efforts to prevent data breaches truly keeping pace with the escalating threat?

We need to approach the problem with fresh eyes—ready to challenge existing assumptions and explore creative solutions. Ask a cybersecurity expert today about their top priorities, and you will hear them discuss areas such as zero-trust frameworks, employee education, and incident response. However, the idea of fortifying the data itself is noticeably absent from many “top five” lists. This raises a critical question: in a world where every system is eventually breachable. This raises a critical question: why aren't more organizations placing the protection of the data itself at the forefront of their strategy? Perhaps it's time to expand our perspective and approach defence in depth from both ends: perimeter-in and from the core outwards.

Most are still approaching it from a perimeter-in approach, focusing their investments on network security, endpoint security, IAMs, etc.

Proportionally, we have witnessed a heightened recognition of the need to improve the security posture and the protection of information assets. There has been an explosion of technological innovations to help safeguard our information assets, especially in today's work-anywhere, always-connected, agile, and hybrid computing world. However, the effort

seems to focus mostly on network security, endpoint security and identity access management.

For decades, information assets were primarily stored as structured data in database systems physically located inside secured data centres. The modality of a medieval castle defence served as an excellent analogy for data protection – establishing strong perimeter defence, employing competent guards to interrogate and validate the identity and the permission of those who wish to access, and ensuring they are not already comprised. Today, we are dealing with both structured and unstructured data (i.e. documents, spreadsheets, emails, etc.) containing sensitive information subject to various regulatory compliance requirements scattered all over the enterprise global computing ecosystem: on-premises in the corporate offices and employee home offices, end-user work and personal devices (both managed and unmanaged), cloud platforms (sanctioned and unsanctioned), and SaaS applications.

The rapid adoption of a cloud-first strategy for enterprise applications further complicates this. Due to the complexity of software and cloud technologies, developers may unintentionally create vulnerabilities in the enterprise data protection framework. No, I'm not talking about the quest for secure software development - I'm referring to the separation of production data from test data, sanitization and protection of the test data, and extending protection to the data that the cyber team might not know about (e.g., cloud storage under unofficial cloud tenets).

Hence, there has been a rise in [Data Security Posture Management \(DSPM\)](#) and [Attack Surface Management \(ASM\)](#) products to expose data and data assets. However, a holistic



approach is needed to address the unstructured and shadow data across the entire organization's technology ecosystem (e.g. beyond the top three cloud providers and the most common SaaS applications) and to add the context (i.e. data owner, intended use, data classification, etc.) of the data it discovered/protects. Leveraging AI/ML capabilities to automatically classify discovered data helps automate aspects of data discovery. Additionally, an iterative interview approach with cross-functional stakeholders to contextualize the results will ensure that the best results are achieved.

In their report, IBM found that the average cost of a data breach jumped to USD 4.88 million in 2024, a 10% spike from 2023 and the highest increase since the pandemic. A rise in the cost of lost business, including operational downtime, lost customers, and cost of post-breach responses, totalled USD 2.8 million, the highest over the past 6 years. It's clear that the typical approach, despite increased investment and technological innovations, hasn't yielded the desired results.

An inside-out approach designed to incorporate reasonable and contextual security controls across the data lifecycle.

Let's consider a data-centric approach that applies security controls to how the information assets are collected, where they are stored, and how they are used and managed.

- 1. Discover:** Establish a comprehensive inventory of data assets, identifying ownership and classification.
- 2. Analyze:** Evaluate existing controls and their effectiveness against the classification of data.
- 3. Protect:** Implement robust security measures such as access control, data encryption, and tokenization.



4. Validate: Regularly assess the adequacy of controls and make necessary adjustments.

5. Monitor and Manage:

Continuously oversee the security landscape, ensuring rapid incident response.

This systematic approach enhances security and aligns with regulatory compliance and risk management objectives, thereby safeguarding the organization's reputation.

DISCOVER

You can't protect what you don't know. The first step is to establish an inventory of data assets that your organization collects, process, and stores and answer the following questions:

- Who owns the data?
- What types of data do we have?
 - Structured data in a database, files, emails, paper files, etc.
- Where does this data come from?
 - End-users, employees, HR, financial systems, R&D, 3rd party systems, etc.
- Where is this data stored?
 - Personal devices, in the cloud, or on servers controlled by the organization. It will help identify potential vulnerabilities and areas for improvement in data security.

How can we classify this data?

- PII, healthcare, financial, PCI, etc.

How can we see what happens to this data over its lifecycle?

- Who/how it would be used, intended retention, destruction, etc.

As we inventory the information assets, we should also classify the data according to their sensitivity, criticality, value, and regulatory compliance ratings. This ensures the ability to apply controls uniformly and consistently downstream. In addition to data inventory, we should examine what controls have been implemented for each asset. This concludes the Discovery phase of the approach.

ANALYZE

The next step is to analyze the controls against the data classification to determine whether they are sufficient and robust. There are quite a few tools that we could leverage for the analysis — CIS Critical Security Controls (CSC), NIST Cybersecurity Framework (CSF), etc. Personally, I prefer a holistic approach that overlays the Capability Maturity Model (CMM) on top of the technical prescriptive nature of CIS CSC and the breadth of NIST CSF. NIST CSF is the most adopted industry standard for cybersecurity and maps very well to most (if not all) compliance and risk management frameworks. The result of the analysis can be refactored into the organization's Enterprise Risk Management (ERM) or Enterprise Security Risk Management (ESRM) process for alignment and SLT support.

PROTECT

Common data protection controls include access control (i.e., access should only be provided to specific job roles, on specific types of data, from specific endpoints, and at specific times), data encryption (i.e., to



prevent unauthorized users from accessing the data even if they have access to the infrastructure hosting the data, such as the file directory, database, email store, etc.), and data tokenization (i.e., making the data usable for some business processes without exposing it). There are technology solutions, like IBM's Guardium for example, that would accomplish them in a manner that works with most existing business processes and minimizes the burden on the end-users (especially if data classification/labelling is done). In addition, it is vitally important to establish key data management processes, such as data retention and destruction policies. The most important thing here is to ensure the investment level for data protection aligns with the organization's ERM/ESRM program. Sometimes, it can be more straightforward and more economical to transfer the bulk of the risk to a 3rd party (e.g. cyber insurance underwriter, business process outsourcer, etc.) and focus on residual risk internally.

VALIDATE

Now that we have completed the data discovery, assessed existing controls for adequacy, and implemented additional controls to bring the safeguards to an acceptable level, we need to ensure a cadence for repeated evaluation. This will ensure that the controls remain effective despite technological, organizational, and threat landscape changes and that new data assets (especially those not stored in the centralized data management solution, or Shadow Data) are incorporated into the established data protection program. In addition, there needs to be a process for regularly reviewing and auditing access to the data.

MONITOR AND MANAGE

Lastly, data security incidents (e.g., policy violation, suspected misuse, data breach, etc.) must be monitored and responded to 24/7, 365 days a year. Incorporating artificial intelligence (AI) and machine learning (ML) to detect abnormal data usage would greatly improve detection efficacy while reducing unnecessary burdens on the team due to false positives. It makes sense to integrate this critical function with the organization's existing security

incident-handling program to take advantage of its around-the-clock coverage model and matured incident management and incident response process.

Reduce the impact of data breaches with a process that aligns with business processes, regulatory compliance and enterprise risk management.

The urgency of enhancing data protection measures is more evident than ever. The combination of escalating cyber threats and the significant financial ramifications of data breaches necessitates immediate action. By adopting a proactive, data-centric strategy, organizations can mitigate risks, reduce impact, and protect their most valuable assets.

What is that proactive data-centric approach and how can you get started, you ask? Lean into an "inside-out" approach to your program, with a good first step being to execute a [Data Security Assessment](#) that focuses on discovering your critical data, or at least a subset thereof. Take an "agile" or iterative approach to Discovery, so that you do not get bogged down by trying to discover *all of your data or all of your critical data*. Discover a tranche of your critical data, then follow the process outlined to Analyze, Protect, Validate, Monitor and Manage. Learn from the first data tranche and then rinse and repeat.

Once started, the contextual insights gained and alignment to various industry frameworks make it far easier to gain senior leadership buy-in and support to sustain this for years to come. Finally, the ability to convey data security in the context of business processes, regulatory compliance and risk management language would surely enhance the level of engagement of business executives. ☺

[Christopher Lee](#) works at Glasshouse Systems and has over twenty years of extensive experience in cybersecurity, concentrating on advanced threat detection and ensuring that client organizations strategically align their capabilities with their unique risk tolerance. He is a recognized subject matter expert in advanced Security Operations Center (SOC) services and cybersecurity advisory services.



Building Resilience Through Cybersecurity Awareness

by [Junior Williams](#)

The Growing Cost of Cyber Threats

In today's digital age, cyber threats have become an unavoidable reality. Building resilience against these threats is critical for navigating an increasingly interconnected and challenging digital environment. The global average cost of a data breach reached \$4.88 million in 2024, marking the largest yearly increase since the pandemic ([IBM Report](#)). This stark reality sets an urgent tone for organizations of all sizes. With most communication and financial transactions conducted online, it's essential for everyone to understand the basics of cybersecurity, regardless of their technical background. The boundaries between personal and business cybersecurity are increasingly blurred. A lapse in

individual online safety can have cascading effects on organizational security, just as a company's weak cybersecurity practices can jeopardize personal data. This interconnected reality demands constant vigilance and proactive measures from everyone to navigate an ever-evolving and complex digital ecosystem.

Personal Cybersecurity: A Vital Life Skill

On a personal level, staying ahead of online threats requires learning new skills. For example, deepfakes—AI-generated videos that impersonate real people—can trick individuals into believing false information or even transferring money to scammers. Hands-on training becomes

invaluable for building practical knowledge and confidence in recognizing and avoiding these evolving threats. This training should be tailored to individual behaviors and digital habits. For instance, users could practice identifying phishing emails, avoiding suspicious links, or managing strong passwords to mitigate common personal cyber risks.

According to Verizon, 68% of breaches involved a non-malicious human element, such as falling victim to a social engineering attack or making an error. This statistic highlights the critical role of individual awareness and education in reducing cyber risks. Websites like TryHackMe offer fun, interactive lessons that help learners at all levels improve their cybersecurity awareness and skills. For instance, the free TryHackMe room 'Web Application Basics' explores topics such as HTTP, URLs, request methods, response codes, and headers, making it an excellent starting point

2.3%

of breaches involved a non-malicious human element, such as falling victim to a social engineering attack or making an error.

for understanding web-related cybersecurity concepts. Similarly, their 'Introduction to Ethical Hacking' room guides learners through the basics of penetration testing and understanding system vulnerabilities, providing a practical foundation for tackling real-world security challenges. Just like learning to drive or manage money, understanding how to stay safe online is a vital life skill.

Tailored Business Training and Leadership in Cybersecurity

The EY 2023 Global Cybersecurity Leadership Insights Study (EY Report) found that only one in five Chief Information Security Officers (CISOs) and C-suite leaders

consider their approach effective for the challenges of today and tomorrow. This statistic highlights the urgency for leadership to adopt more forward-looking strategies to address the evolving threat landscape.

For businesses, cybersecurity awareness needs to be continuously updated. One-off training sessions every year aren't enough because cyber threats are constantly evolving. To address this, organizations must invest in dynamic training methods that engage employees meaningfully and regularly. Role-based gamified training modules, which use game-like elements to simulate real-world scenarios tailored to specific roles, can make this approach more impactful. For example, an employee in customer support could engage in a simulation where they must manage a sudden surge of customer complaints linked to a fake website impersonating their company, a scenario tailored to their daily interactions, while IT staff might navigate a module designed to detect unusual network activity in real time. This personalized approach ensures that training resonates with users, making it both relevant and actionable.

Training should go beyond avoiding scam emails and focus on role-specific threats and responsibilities. For instance, employees in finance should learn about risks such as fraudulent invoices and wire transfer scams, while HR staff might explore vulnerabilities tied to sensitive employee data. Tailored training ensures that cybersecurity feels relevant and actionable, fostering deeper employee commitment to organizational safety.

Additionally, the new Govern function in NIST CSF 2.0 underscores cybersecurity as a critical enterprise risk. Senior leadership is now expected to prioritize it alongside financial and reputational considerations. By extending its guidance beyond critical infrastructure to all organizations, this framework highlights the necessity of universal cybersecurity vigilance, irrespective of an organization's current level of cyber maturity.

Technology as a Cybersecurity Ally

New technologies are also making cybersecurity education easier and more personalized. AI-powered chatbots are transforming learning by offering interactive and tailored educational experiences. For instance, you could ask an AI, "Create a five-question quiz about cybersecurity and provide a lesson based on my answers." This kind of interaction makes learning more engaging and accessible for everyone, from executives to new hires. Importantly, this approach is not confined to cybersecurity; it can extend to topics like programming or financial literacy. Organizations can use these tools to build



cross-functional skills across teams, preparing individuals to navigate diverse challenges. For example, employees might utilize similar AI-driven platforms to explore supply chain risk management or improve strategic decision-making, creating a more adaptable and capable workforce.

Such technologies play a transformative role in industries like financial services, where the stakes for cybersecurity are particularly high. Data breaches in this sector can compromise sensitive financial information, disrupt operations, and result in regulatory penalties. According to Varonis ([Financial Data Risk Report](#)), financial services take an average of 233 days to detect and contain a data breach. This prolonged timeframe—equivalent to over eight months—allows attackers ample opportunity to exploit vulnerabilities, damaging reputation, revenue, and customer trust. By leveraging AI tools that provide real-time threat analysis and integrating these with comprehensive awareness training, organizations can not only shorten response times but also anticipate and prevent future breaches. This proactive approach ensures a more resilient security posture, critical in an environment where agility and foresight are essential.

Building a Culture of Cybersecurity

Cybersecurity awareness hinges on adopting the right mindset, both personally and organizationally. This means fostering habits like regularly questioning the legitimacy of unexpected communications, staying informed about emerging threats, and taking proactive steps to strengthen defenses. For example, an individual might develop the practice of verifying unusual requests through alternate channels, while organizations could encourage team discussions about recent phishing tactics to build collective awareness.

Human error accounts for more than 80% of cyberattacks, according to the National Institute of Standards and Technology ([NIST Blog](#)). This underscores the importance of cultivating habits like questioning unexpected messages, staying curious about potential threats, and proactively seeking knowledge about emerging risks. Building resilience against cyber threats starts with fostering a culture that emphasizes continuous learning and open communication across all levels.

To move forward, organizations and individuals must actively invest in their cybersecurity education and practices. Whether by adopting advanced technologies, implementing tailored training programs, or reinforcing everyday vigilance, the goal is clear: build a resilient and secure digital environment. Now is the time to act—start by evaluating your current approach and taking steps to strengthen your defenses today. It's not just about memorizing a set of best practices. It's about staying informed and proactive. For organizations, this means embedding cybersecurity into the culture and ensuring every employee understands their role in maintaining security. It's about recognizing the connection between our actions—at home and at work—and the broader digital world. With the right tools and regular updates, cybersecurity learning can become an active, engaging part of daily life. ⁸

Junior Williams, a seasoned cybersecurity and AI professional with a wealth of experience in programming, technology, investigations, and consulting, has built an extensive career marked by adaptability to the rapid pace of technological advancements. His expertise has evolved from telecommunications to IT infrastructure, where he developed a deep understanding of computer systems, cybersecurity, and the strategic implementation of AI solutions to drive impactful business outcomes.



Your Trusted IAM Partner:
**Strategy, Implementation,
and Managed Services, all
in one place.**

IAM | PAM | CIAM

www.iamconcepts.ca | info@iamconcepts.ca





Securing Digital Identity in an AI-Driven World

by [Fahad Kabir](#), Presented by IAMConcepts Security Solutions Inc.

The advent of artificial intelligence (AI) has profoundly impacted numerous industries, and identity security is no exception. Generative AI, in particular, is revolutionizing the way organizations approach Identity Governance and Administration (IGA), Identity Threat Detection and Response (IDTR), and overall identity lifecycle management. As the field evolves, the integration of AI promises not just efficiency but also meaningful innovation that redefines user interactions and organizational security.

Generative AI: Transforming Identity Governance

Generative AI is emerging as a game-changer in identity management, addressing longstanding challenges in IGA.

One of the primary hurdles for IGA adoption has been access certification fatigue. Employees often resort to “rubber-stamping” approvals, bypassing the intended security checks. Similarly, role mining and role engineering have been persistent pain points, requiring vast amounts of data to identify meaningful patterns and ensure the right levels of access.

By leveraging generative AI, organizations will soon be able to process large datasets more effectively and derive actionable insights. For instance, an IGA tool powered by generative AI will be able to recommend roles and access levels based on historical data, risk patterns, and organizational policies. A lot of this AI powered analysis capability were available in leading IAM tools before. However, the

differentiator going forward will be making these tools much more user friendly and interactive by leveraging generative AI. This capability simplifies the decision-making process, allowing users to ask intuitive questions such as, “What type of access should this new hire have?” or “What risks are associated with this role?” Such user-friendly interfaces, akin to interacting with ChatGPT, eliminate the need for end-users to possess technical expertise, democratizing access to identity tools.

AI-Powered Enhancements by IAM Product Vendors

Leading Identity and Access Management (IAM) product vendors are embedding AI fast into their solutions to deliver more intelligent and efficient identity and access management. These enhancements include:

- 1. Automated Role Mining and Engineering:** Vendors are incorporating AI to analyze access patterns, suggesting optimal role structures, and simplifying the often tedious process of role engineering.
- 2. Intelligent Access Certification:** AI-powered solutions reduce certification fatigue by identifying high-risk access points and prioritizing them for review, streamlining the approval process.
- 3. Adaptive Risk Assessment:** AI is being used to continuously evaluate risk in real-time, factoring in user behavior, location, and device to provide dynamic access decisions.
- 4. Enhanced Threat Detection:** Vendors are leveraging machine learning algorithms to detect anomalies, flag suspicious activities, and provide actionable insights to security teams.
- 5. Privileged Account Discovery and Protection:** Identifying privileged accounts across any large enterprises has been a challenge in the industry. AI powered modern PAM tools will be much more advanced in scanning an organization’s entire network efficiently, continuously analyzing and identifying privileged accounts that might not be explicitly documented.

These innovations not only improve security but also enhance usability, making IAM solutions more intuitive and effective for organizations of all sizes.

Redefining User Experience

One of the most significant benefits of AI in identity management is enhancing user interactions. Traditional identity

tools often require specialized training, creating friction between end-users and the technology. Generative AI flips this paradigm by making interactions more conversational and intuitive. For example, instead of navigating complex interfaces, users can pose natural language queries to the system. This shift not only increases adoption rates but also ensures that identity management becomes a seamless part of daily operations.

Imagine an HR professional onboarding a new employee. Instead of manually navigating the labyrinth of access permissions, they could simply ask, “What are the appropriate access permissions for a junior analyst in the marketing team?” The system, leveraging generative AI, would analyze existing roles, assess potential risks, and offer tailored recommendations. This streamlined approach empowers organizations to maintain security without overburdening users.

One of the most significant benefits of AI in identity management is enhancing user interactions.

AI’s Role in Identity Threat Detection and Response

Identity Threat Detection and Response (ITDR) is a critical evolution in cybersecurity, as traditional tools like SIEM and EDR have primarily focused on broader security events and logs, often overlooking the vital context of identity data. With cyber threats becoming increasingly sophisticated, leveraging identity-specific data has become essential for accurately detecting and mitigating risks. ITDR focuses on the behaviors and activities tied to user identities—such as login patterns, access permissions, and authentication methods—to identify anomalies that might indicate malicious activity or compromised accounts. Modern cybersecurity tools are starting to integrate ITDR



capabilities by incorporating advanced AI and machine learning, which can analyze vast amounts of identity data in real-time. These tools can detect deviations like logins from unusual locations, sudden privilege escalations, or unauthorized access attempts, enabling more precise and timely responses. By blending identity-specific monitoring with traditional security frameworks, organizations can strengthen their overall security posture, ensuring a more holistic approach to threat detection and response. This integration ensures that identity-related risks are addressed as a core part of an organization's broader cybersecurity strategy.

Organizations must embrace a collaborative approach, leveraging both cutting-edge technology and expert guidance.

Market Leaders and Professional Services

Most product vendors are already integrating AI into their solutions, setting the stage for a competitive landscape in identity management. However, deploying these advanced tools requires more than just technical expertise and professional services will continue to play a crucial role in ensuring meaningful implementation.

Even with AI-powered tools, organizations will require guidance to tailor these solutions to their specific needs. Professional services help connect

disparate systems, customize features, and train users, ensuring that deployments achieve their intended outcomes. The ultimate goal is to make identity tools as intuitive as consumer-grade applications, allowing users to focus on decision-making rather than the mechanics of the system.

The Path Forward

As AI continues to evolve, the future of identity security looks promising. Generative AI has the potential to address some of the most pressing challenges in IAM, IDTR and beyond. By simplifying complex processes, enhancing user experiences, and delivering actionable insights, AI is redefining the role of identity in modern organizations.

To fully realize these benefits, organizations must embrace a collaborative approach, leveraging both cutting-edge technology and expert guidance. The evolution of identity in the age of AI is not just about automation; it's about empowering users, enhancing security, and driving innovation. 🌐

Fahad Kabir is the CEO of IAMConcepts Security Solutions Inc., a cybersecurity professional services firm specializing in digital identity and access management for businesses. With over 20 years of experience leading consulting organizations, he has a proven track record of delivering outstanding results across various industries. Before joining IAMConcepts, Fahad held leadership roles at global consulting firms including EY, Accenture, and Deloitte. He is recognized as a visionary and thought leader in the cybersecurity industry, having spoken at numerous global conferences on topics such as the future of Identity & Access Management, cyber threats in the financial industry, and security program management.



The Canadian Threat Landscape by Julien Richard

Digital technology powers every aspect of Canadian society—from healthcare and critical infrastructure to small businesses and government services. As organizations become more connected and dependent on technology, they also become more vulnerable to an evolving array of cyber threats. These aren't just technical challenges; they represent real risks to essential services, economic stability, and public safety. As cyber threats continue to evolve, state-sponsored activities stand out as one of the most significant concerns facing Canadian organizations and institutions.

State-Sponsored Threats

State-sponsored cyber operations against Canada continue to intensify and evolve beyond traditional espionage. According to the Canadian Centre for Cyber Security's [National Cyber Threat Assessment 2025-2026](#), state

adversaries are becoming more aggressive in cyberspace, attempting to cause disruptive effects such as denying services, deleting or leaking data, and manipulating industrial control systems. The CCCS states in the report that China, Russia, and Iran remain primary concerns, while India has emerged as a new threat amid diplomatic tensions. These state actors have shifted their tactics, often compromising domestic infrastructure like home and small office routers to mask their activities. This approach proved devastating when attackers breached [Global Affairs Canada's VPN](#), maintaining access for over a month and potentially exposing classified information. Even more concerning, state-sponsored actors now very likely consider civilian critical infrastructure as legitimate targets for cyber sabotage in the event of military conflict. Along with state-sponsored threats, ransomware has emerged as one of the most pervasive and damaging forms of cyber attacks.

Ransomware Trends

Ransomware attacks remain a dominant cyber threat in Canada. According to [Mandiant](#), the median dwell time for ransomware attacks dropped to just 5 days in 2023, underscoring attackers' efficiency. Victims are frequently forced into ransom payments to regain access to data, although many organizations now prioritize incident response over paying attackers. Despite this, ransomware tactics continue to evolve, with attackers increasingly targeting sensitive business operations rather than just data encryption. The impact of these and other cyber threats is amplified by the dramatic increase in attack sophistication and speed.

Evolution of Attack Sophistication

The sophistication and speed of cyberattacks have increased dramatically in recent years. According to [Mandiant's 2024 analysis](#), the window between a vulnerability's discovery and exploitation has shrunk from 63 days in 2018 to just 5 days in 2023. Even more alarming is that 12% of vulnerabilities are now exploited within 24 hours of discovery. The [MOVEit attack](#) campaign of 2023 demonstrated this rapid exploitation, affecting more than 2,700 organizations and compromising over 93.3 million individual records globally. In Nova Scotia alone, 100,000 people were affected, costing the province [\\$3.8 million](#) in response efforts. These sophisticated attacks have particularly severe impacts on critical sectors of Canadian society.

Sector-Specific Impacts

The healthcare sector has proven particularly vulnerable to these evolving threats, especially ransomware and state-sponsored activity. In 2023 alone, the sector faced [630 ransomware attacks](#) globally. Healthcare data breach expenses have surged by 53.3% since 2020, with system downtime alone costing medical organizations an estimated \$15.5 million in 2023. The [Toronto Hospital for Sick Children](#) ransomware attack demonstrated the sector's vulnerability, disrupting patient care and lab results.

Critical infrastructure faces an equally concerning threat from cyberattacks. Between January 2023 and January 2024, these vital systems experienced over 420 million attacks globally, averaging 13 attacks every second, as reported by [Security Today](#). The utility sector has been especially targeted, with cyberattacks increasing by 70% compared to 2023, according to [U.S. News](#). This sharp rise is linked to growing digitization and reliance on outdated systems, leaving critical components vulnerable to exploitation.

Emerging technologies are also creating new points of attack, fundamentally reshaping the nature of cybersecurity challenges in these sectors.

Emerging Threats

Attackers now leverage AI to enhance phishing campaigns, generate convincing deepfakes, and analyze stolen data with unprecedented efficiency. They create [sophisticated fake news websites](#) posing as local outlets while using AI-powered analytics to identify and target victims with precision. The rising value of cryptocurrency, with Bitcoin up 133% in the past year to over 125,000.00 CAD, has coincided with increasingly expensive ransomware demands. According to [Sophos' State of Ransomware 2024](#) report, the median ransom payment has increased five-fold from the previous year to \$2,000,000 USD, while the mean payment reached nearly \$4,000,000 USD. Particularly concerning is that 63% of ransom demands are now for \$1 million or more, with 30% demanding \$5 million or more. The surge in cryptocurrency values has not only increased the potential payout for attackers but has also provided them with a larger pool of resources to fund sophisticated operations.

\$2.3 million

is the average recovery cost on Canadian organizations, excluding ransom payments.

The impact on Canadian organizations is significant, with recovery costs averaging \$2.73 million in 2024, excluding ransom payments. This represents an increase of almost \$1 million from the previous year. The cryptocurrency connection is particularly relevant as ransoms are typically paid in cryptocurrency, making the rising values of digital currencies a direct multiplier of cyber risk.

Quantum computing presents a looming threat to current cryptographic standards. [Canada's 2022 National Quantum Strategy](#) emphasizes the urgent need to prepare, with federal quantum readiness assessments suggesting that 2026

could mark the earliest possible quantum threat to current encryption methods.

Social media use also presents significant risks, both in terms of privacy and security. According to [Statistics Canada](#), over 70% of Canadians aged 15 and older reported experiencing a cyber-related incident in 2022. Addressing these evolving threats requires not only technological solutions but also a skilled workforce capable of implementing and maintaining robust cybersecurity measures.

70%

of Canadians aged 15 and older reported experiencing a cyber-related incident in 2022.

Workforce and Skills Gap

The cybersecurity challenges facing Canadian organizations are compounded by a significant workforce shortage. According to the [Information and Communications Technology Council's Digital Talent Outlook for 2025](#), Canada will need an additional 250,000 digitally skilled workers by 2025, with the digital economy expected to employ 2.26 million workers—approximately 11% of all employment in the country. This shortage is particularly acute in cybersecurity roles, where specialized skills are essential for protecting critical systems and data. The skills gap is especially challenging in sectors like advanced manufacturing and healthcare, which are projected to need 14,000 additional workers each by 2025, while also facing increasing cyber threats.

Canadian Legislation

To address the growing complexities of cybersecurity, Canada has introduced key legislative measures aimed at safeguarding critical infrastructure and protecting Canadians online. However, these initiatives are not

without their challenges and have drawn criticism for their potential implementation hurdles and broader implications.

[Bill C-26, the Act Respecting Cyber Security](#), represents Canada's first comprehensive attempt to protect critical infrastructure through cybersecurity legislation. It creates new obligations for operators in telecommunications, finance, energy, and transportation sectors, requiring them to implement cybersecurity programs and report incidents to the Canadian Centre for Cyber Security.

[Bill C-63](#) addresses social media and online risks by enhancing protections against cyberbullying and online harms while also implementing a framework for reporting and investigating these incidents. These measures align with the bill's broader goal of ensuring a safer digital environment for Canadians. The financial implications of these cyber threats extend across all sectors, resulting in significant economic impact for Canadian organizations and governments.

Economic Impact

Cybercrime continues to cost Canadian organizations billions every year. The [Canadian Centre for Cyber Security](#) estimates that the economy lost \$9.7 billion in 2023 due to these threats. Industries like healthcare, manufacturing, and finance often feel the biggest impact because they rely so heavily on technology and can't afford disruptions. For example, the [City of Hamilton](#) faced \$7.4 million in recovery costs after a cyber attack, with another \$30 million needed to strengthen its defenses.

The financial damage doesn't stop at direct costs. Cyber incidents can lead to lost customers, downtime, and higher insurance premiums, which all add up quickly. For industries like healthcare and finance, a breach doesn't just disrupt operations—it can erode trust with patients and clients, making recovery even harder. Add in the cost of legal fees and regulatory fines, and it's clear these threats have widespread implications for organizations and the economy as a whole.

Future Outlook

Cybercriminals are shifting their focus from merely encrypting data to targeting its integrity, manipulating critical records such as financial ledgers, medical diagnoses, or operational parameters to coerce victims into paying ransoms to restore accuracy. This emerging tactic, as highlighted by the [IBM Security X-Force Threat Intelligence Index 2024](#), undermines trust in organizational systems and creates

complex challenges for detection and recovery, beyond traditional ransomware attacks. The report also reveals an alarming shift in attack methods, with deployment time for ransomware attacks dropping from less than two days to less than four hours, and notes that manufacturing has become the most attacked industry for the third consecutive year. To counter these threats, organizations must prioritize data integrity monitoring and robust recovery processes to ensure the authenticity of their information.

The path forward...Requires integrating security into every business decision, investing in both technology and training , and preparing for threats that have yet to emerge.

The rise of connected and autonomous vehicles (CAVs) presents new cybersecurity challenges for Canada's transportation infrastructure. The integration of digital systems in vehicles and networks creates vulnerabilities that malicious actors can exploit. Transport Canada's [Vehicle Cyber Security Guidance](#) highlights the risks posed by interconnected supply chains, while the [Canadian Centre for Cyber Security](#) warns of potential threats throughout the digital supply chain. Studies on LiDAR systems reveal how adversarial attacks can disrupt autonomous navigation, affecting not just vehicles but entire transportation networks. These evolving threats demand robust cybersecurity measures to protect Canada's infrastructure.

As the Canadian Centre for Cyber Security notes, cybersecurity has evolved beyond a mere IT issue to become a business survival imperative. The path forward for Canadian organizations requires integrating security into every business decision, investing in both technology and training, and preparing for threats that have yet to emerge. Success in this environment doesn't require predicting every threat but rather building systems and teams that can adapt, recover, and learn from emerging challenges. Understanding this reality is crucial, but it requires clear action to protect organizations and their stakeholders from persistent cyber risks.📍

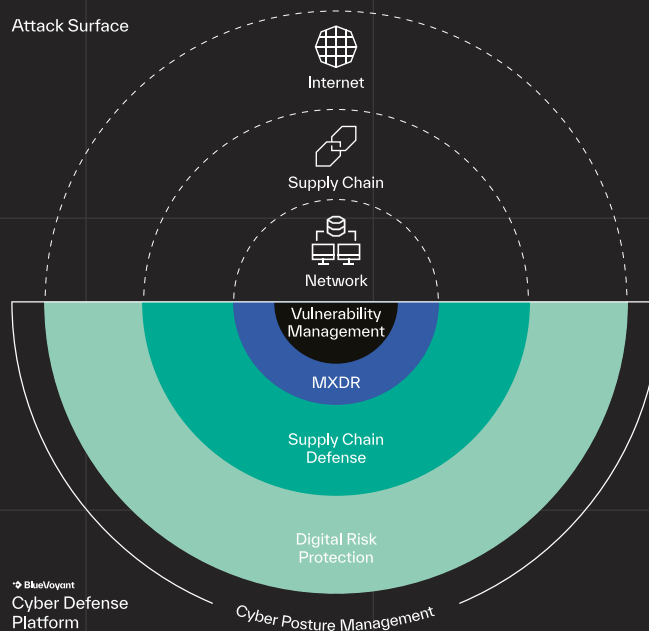
[Julien Richard](#) is the Vice-President of Infosec at Lastwall. Julien also operates BCK Security, a freelance consulting firm.





Cyber Defense Platform

Seamless AI-driven internal, external, and supply chain cyber defense, all within one powerful Security Operations Platform.



BlueVoyant Supply Chain Defense

BlueVoyant Supply Chain Defense is a fully managed solution that identifies, validates, and resolves critical cybersecurity issues in your third-party ecosystem.

Key Use Cases:



Continuous Monitoring & Remediation



Point-in-Time Risk Assessments



Questionnaire Management



Vendor Risk Management & Consulting

Ready to learn more?





The State of Third-Party Cyber Risk Management in Canada

Presented by BlueVoyant

Findings from a recent survey of Canadian C-level executives found a staggering 93% of Canadian organizations have been negatively impacted by a cyber breach within their supply chain in the past twelve months, 10 percentage points greater than global counterparts.

As enterprises become more interconnected and have more suppliers and vendors, Canadian organizations are facing heightened challenges in managing supply chain cybersecurity. BlueVoyant's recent [The State of Supply Chain Defence](#) report revealed 93% of Canadian organizations have been

impacted by a cyber breach within their supply chain, significantly more than the 81% of global respondents who said the same. On average, Canadian companies experienced 3.96 breaches in the prior 12 months, slightly higher than the global average of 3.68.

Vendor and Supplier Monitoring Practices

Canadian organizations have large vendor networks with the most common number of vendors being somewhere from 1,001 to 10,000 vendors (35%). Yet, most

organizations say they only evaluate 501 to 1,000 of them for cyber risks (39%). Thirty-six percent of respondents who know how many suppliers they work with say they regularly monitor between 1,001 and 10,000 vendors.

Working with third-party vendors remains a critical area of concern, with only 36% of Canadian organizations saying they engage with such partners, aligning with global figures. Alarming, 31% of these companies say they have no way to detect issues with third-party vendors, a slight increase over the global average of 30%.

Continuous monitoring is most reported solution for third-party cyber risk management, adopted by 32% of Canadian firms. However, many companies say they are only monitoring vendors quarterly (31%).

Canadian organizations are less likely to have continuous autonomous transparency (11% compared to 15% globally), indicating room for improvement in real-time risk assessment.

Budget Increases Reflect Growing Concerns

The silver lining is that things may begin to change with budgets increasing. More than nine-in-ten (92%) of Canadian organizations say they have increased their cybersecurity budgets, compared to 86% globally. This increase in funding reflects a growing recognition of the need for robust defences against third-party cyber threats. Canadian firms are likely to channel these enhanced budgets into both internal (51%) and external (59%) third-party cybersecurity resources, showing demand for both employees skilled in supply chain risk, and vendors to help monitor and respond to supply chain cyber threats.

Improving Canadian Third-Party Cyber Risk Management

The study findings suggest that while Canadian organizations are making strides in supply chain cybersecurity, there is still a critical need for enhanced third-party risk management (TPRM) practices. Increased automation and integration of third-party cyber risk management into broader security and risk operations could provide more scalable and effective solutions.

“More organizations than any previous year indicated that their primary focus is no longer on awareness of the third-party risk management problem or adoption of a program, but rather with the operational, day-to-day challenges of managing an effective program,” said Joel Molinoff, global head of Supply Chain Defence at BlueVoyant. “While this progress also brings many new challenges, it indicates

a major step in the right direction. Since Canadian organizations say they are increasing budgets, we will hopefully see them implement more best practices to better monitor their digital supply chains, and work with third parties to quickly mitigate any issues.”

The importance of analyst-driven decision making and having a “human in the loop,” cannot be understated.

To help improve Canadian third-party cyber risk management, organizations should consider increasing automation. As with many other business functions, supply chain cyber risk management will continue to see increased reliance on automation and AI as a way of making effective risk management more accessible and scalable, especially for smaller- and medium-sized organizations that struggle with personnel and resource limitations.

At the same time, it has become evident that complete automation is not a viable solution. The importance of analyst-driven decision making and having a “human in the loop,” cannot be understated, especially for aspects of solutions like following up with third parties to ensure effective remediation.

As information security as an industry continues to mature, there will be more focus put on the integration of various aspects of security operations. This means that third-party cyber risk will inevitably be folded into day-to-day SOC operations and wider risk management programs.

As Canadian companies continue to navigate the complexities of supply chain cybersecurity, the focus must remain on proactive identification and working with vendors to mitigate vulnerabilities quickly. Ⓔ

The research was conducted by Opinion Matters, with a sample of 74 CTOs/CSOs/COOs/CIOs/CISOs/CPOs responsible for supply chain & cyber risk management working in companies employing 1,000+ employees in Canada. The data was collected between 20.08.24 - 29.08.24 Opinion Matters abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Opinion Matters is also a member of the British Polling Council.



Cybersecurity for Canadian Digital Infrastructure

by [Albert Heine](#)

Introduction

In this article we are going to focus on the cybersecurity of digital infrastructure that powers Canadian businesses and government institutions. The goal is to understand where technology trends are heading towards, the associated risks, and how it relates to other, more broad cyber-risks. Based on that, a focused set of mitigation strategies related to infrastructure is proposed that should help future-proof the majority of Canadian businesses.

Since the term “digital infrastructure” is broad and can mean a variety of different combinations of technologies, we are going to highlight in the first section what the trends are when setting up infrastructure to power modern applications.

Furthermore, we are going to look at Canada’s Information, Communications and Technology (ICT) sector and take into account unique properties and their effect on the adoption of technology and choice of digital infrastructure.

After the outline on the focus-areas of digital infrastructure, we are going to describe the most common risks and misconceptions. For each risk, we are going to discuss the most established mitigation strategies. This provides a clear picture of what could and should be prioritized today in your organization.

We are going to finish this article with a subsection on future trends and how to be prepared for them.

Digital infrastructure in Canada

Similar to trends observed on a global scale, Canada's cloud adoption has reached 48.5% in 2023,¹ and is steadily growing across all enterprises. When focussing on the ICT sector, 95.5% of all companies in this sector are under the category of "Software and Computer services", and most of ICT companies (84.9%) have less than 10 employees.² Hence, one can assume that the cloud adoption among ICT companies in general is likely much higher than the overall number across all enterprises.

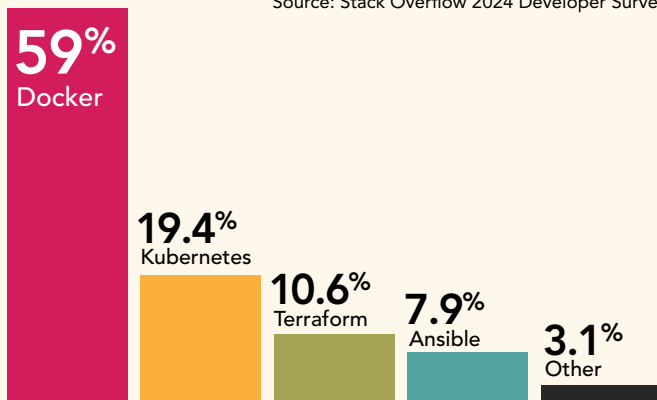
In addition to the private enterprise sector, Canada is itself committed to moving their infrastructure steadily to the cloud since 2018.³

For these reasons, cloud-related risks should be considered a major focus when considering cybersecurity of Canadian digital infrastructure.

In addition to that, one needs to also study which technologies are employed in the cloud, to further refine the overall image of infrastructure related tools. While there is no country-specific study available there, the yearly Stack-overflow Developer survey sheds light on technology trends that indicate which technologies are being used by developers. Without surprise, Docker appears to be the No. 1 technology with over 59% of Developers using it. It has transformed the way we are building and deploying code on any infrastructure, and draws the bridge between development and IT. Further infrastructure related tools are Kubernetes (19.4%), Terraform (10.6%) and Ansible (7.9%).⁴ This leads to the conclusion that containers are the major build and deployment vehicle on infrastructure today, including the cloud, and are growing in the future. The high use of containers compared to the common container orchestration tools leads to the conclusion that the processes, even when containers are involved, remain manual for the majority.

Which technologies are being used by developers

Source: Stack Overflow 2024 Developer Survey



Risks and mitigation strategies

Using the cloud comes most of the time with a general misconception: The cloud provider will take care of the security needs. That belief is very prevalent in Canada, with 31% of Canadian executives holding on to it.⁵ The truth is that there is a shared responsibility model when it comes to utilizing the cloud (see e.g. the respective articles by [AWS](#), [Azure](#) and [GCP](#)).

Hence, it is important for any team using cloud technology to understand the risks for any utilized service. And that awareness only covers the layer of the cloud itself. Container orchestration, container security measures and third party application security have to be considered as well. For the longest time, cloud security posture management was the sole focus, but the latter mentioned application configuration security is now also starting to come into the spotlight with the latest revision of the FedRamp security framework,⁶ where DoD Stigs and other benchmarks require a monthly report. FedRamp is usually the first framework that adopts new control criteria historically, and others tend to follow.

One of the reasons for this shift can also be directly correlated to the cybersecurity situation in Canada. According to the "Baseline cyber threat assessment: Cybercrime" report by the Canadian Center for Cybersecurity,⁷ "ransomware [is] almost certainly the most disruptive form of cybercrime that Canadians face and has significant impacts beyond the financial cost of the ransom itself." According to a study by Microsoft,⁸ 80% of ransomware attacks can be traced to misconfigurations in devices and operating systems. Hence, infrastructure security should be seen as the highest priority when trying to prevent ransomware attacks.

In addition to handling misconfigurations, on premise, or on the cloud, or inside containers: Canadian organizations will need to be able to update in case of a common vulnerability and exposure (CVE), and they need to be able to update fast. This ability is crucial to avoid keeping doors open for potential attackers. The best known mitigations against that are known as the DevSecOps process and the use of infrastructure-as-code as much as possible. In this way, your teams can update fast and with confidence, since change management is automated and tested properly. At the same time, misconfigurations and code quality can also be re-assessed with every change and deployment.

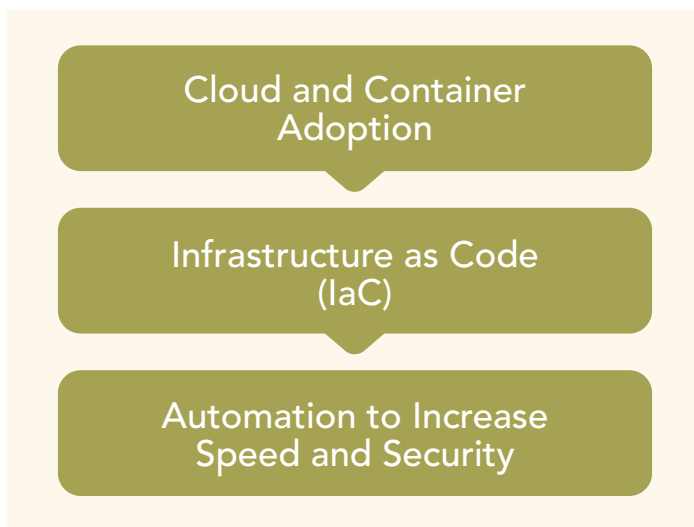
May it be called DevSecOps or any other newly emerging term, at its core is one underlying principle: Automation. The more infrastructure processes can be automated, and the more these automations follow commonly established

standards, the more flaws, vulnerabilities and misconfigurations can be caught in an organization, and the more straightforward will be any auditing process for compliance purposes.

Red Hat is even going one step further by calling automation now “mission-critical”, and correlates automation efforts, besides the security benefits, with ROI in terms of productivity, efficiency and downtime-reduction.²

Given that, as previously mentioned, most ICT companies in Canada are under 10 employees, the process change towards automation on a large scale is more than feasible. This puts Canada in a unique position by being able to be at the forefront of innovation of business and technology processes.

Classic controls like proper network segmentation and well-defined entry points such as load-balancers also mitigate the risk of attackers reaching sensitive data. While many still view it as the cloud provider’s responsibility, it is not. A proper design and implementation of a network architecture lies with the development team, and also needs to be reviewed and checked regularly.



New technologies and future outlook

This is likely the first technology article you read since 2023 that took more than two pages to mention the words Artificial Intelligence (AI). But here we are.

According to the largest survey in the developer industry, 76% of developers are planning to use AI in their development process⁴. Many other departments such as marketing and customer success experienced a spike in AI tool use since 2023 as well.

But with this new technology, demands for data privacy and IP protection are also coming forward. A principle from

even before the time of LLMs, when most AI-related efforts were targeted at machine learning, remains true:

In the DevSecOps process, one part should be to clearly define a Role Based Access Control (RBAC) architecture, and

There is no AI (artificial intelligence) without IA (information architecture).

—Unknown

this architecture should also control the data access and manipulation flow. If LLM models need to be trained on company data, it is obvious that one needs to ensure that only information that a user actually should have access to is accessible to the user through the LLM. I.e., the training path needs to be clearly defined and isolated. The proper architecture of such multi-models is in its infancy, but at its core, independent of the implementation, there will always be the need to define access rights and an auditable process regarding where, when, and how user-data gets stored and distributed. Especially in Canada and the European Union, where the Personal Information Protection and Electronic Documents Act (PIPEDA) and the General Data Protection regulation (GDPR) are in place respectively, this is something to get right today to be ready for the future.

The aforementioned trends in terms of Infrastructure are providing the necessary functionality to aid this effort: Containers and their orchestration tools, such as Kubernetes, come with a built-in RBAC functionality, and the major cloud providers are allowing for fine-grained access controls on their platforms. Furthermore, a new functionality across all major Cloud and IaC providers called Policy as Code (PoC) is emerging, further assisting developers to enforce policies at all stages of the build and deployment process.

Hence, at the core is automation. Nothing is better documentation about data-flow and access controls than coded automation processes. The more standardized these processes are, the more an organization can rely on automated tools to catch misconfigurations or other problems and significantly reduce their risk of being hacked.⁸

Dr. Albert Heinle is driven by a mission to combat the global surge of data breaches and misconfigurations. Albert co-founded CoGuard in 2020 and serves as Chief Technology Officer. Prior to CoGuard, Albert held development positions at FLIR Systems, Inc., Aeryon Labs and Sortable. He completed a Ph.D. in Computer Science at the University of Waterloo in the area of Symbolic Computation.



The State of Software Supply Chain Security in Canada

by [Dmitry Raidman](#)

Introduction

Software supply chains have become critical targets for cyber adversaries globally, and Canada is no exception. These complex ecosystems, consisting of software developers, vendors, third-party suppliers, and end-users, are vulnerable to sophisticated attacks. [The Canadian Centre for Cyber Security \(CCCS\)](#), through its publication [ITSM.10.071](#), highlights the risks and the steps organizations can take to mitigate these threats. Legislative frameworks like Bill C-26 further underscore Canada's focus on bolstering its cyber defenses by addressing supply chain risks. By comparing Canada's efforts to initiatives in the United States and the European Union (EU), this report provides a comprehensive overview of the current state of software supply chain security.

The Software Supply Chain Threat Landscape

CANADA: GROWING RISKS AND CHALLENGES

In Canada, cyber threat actors increasingly target software supply chains, exploiting vulnerabilities in open-source libraries, third-party dependencies, and trusted vendor relationships. As [ITSM.10.071](#) outlines, these attacks compromise systems by leveraging the trust between software providers and consumers. Examples such as the [Log4j](#) vulnerability or [xz](#) supply chain attack demonstrate how

widely used components can expose organizations to global risks, leading to significant disruptions in Canadian federal agencies and private-sector firms.

KEY THREATS IDENTIFIED BY CCCS:

- **Compromised Updates:** Threat actors insert malicious code during software updates, as seen in the [SolarWinds](#) breach.
- **Open-Source Dependencies:** Widely used libraries often contain hidden vulnerabilities exploited by adversaries to gain persistent access.
- **Vendor Privileges:** Elevated access granted to vendors increases risks, particularly in cloud and SaaS environments.

Global Perspectives: U.S. and EU

In the United States, [Executive Order 14028](#) mandates the adoption of a Software Bill of Materials (SBOM) to improve transparency and address software supply chain vulnerabilities. Published by NIST, the [Secure Software Development Framework \(SSDF\)](#) provides actionable guidance for secure software development and aligns closely with CCCS recommendations. Notably, SBOMs are mandated for all software sold to U.S. federal agencies for companies that develop products that require FDA approval and showcase a commitment to proactive security.

The European Union adopts a regulatory-driven approach through the [Cyber Resilience Act](#), which imposes stringent requirements on software vendors to ensure product security throughout its lifecycle. The EU's emphasis on continuous monitoring and transparency mirrors Canadian and U.S. priorities, indicating a global alignment in combating supply chain risks.

Canada's Approach to Mitigating Risks

LEGISLATIVE AND POLICY FRAMEWORKS: [BILL C-26](#)

Bill C-26, passed on Dec 5, 2024, represents a significant step forward in Canada's efforts to address cybersecurity challenges. It mandates critical service operators to implement comprehensive cybersecurity programs, mitigate third-party risks, and report incidents. By requiring organizations to identify vulnerabilities in their supply chains and enforce rigorous monitoring, the legislation strengthens Canada's overall security posture.

Key provisions related to supply chain security include:

- **Critical Cyber Systems Protection Act:** Operators of vital systems must mitigate supply chain risks, establish cybersecurity programs, and comply with government directives.
- **Telecommunications Security Enhancements:** Directives to secure telecommunications infrastructure include mandates to mitigate third-party risks and adopt security standards.

Adoption of SBOM for Visibility and Transparency

The government regulation highlights the Software Bill of Materials (SBOM) as an essential tool for achieving supply chain transparency. An SBOM provides an inventory of software components, enabling organizations to:

1. **Identify Vulnerabilities:** By mapping dependencies, organizations can quickly detect components affected by newly discovered vulnerabilities, reducing the MTTD and MTTR.
2. **Enhance Collaboration:** Sharing SBOMs between vendors and clients facilitates better risk assessment and remediation.
3. **Enhance Asset Risk Management:** Linking between SBOM data and assets management solutions by the end users will provide end-to-end operationalization of SBOMs.
4. **Streamline Compliance:** Aligning with regulatory frameworks like Bill C-26, FDA, and U.S. federal mandates like EO 14028 ensures compliance and strengthens overall security.

COMMON TYPES OF SBOMS:

BOM Type	Definition	Purpose
SBOM	Software Bill of Materials	Provides an inventory of all software components in a product, enabling vulnerability detection and transparency.
AIBOM	Software Bill of Materials for AI	Identifies AI models, datasets, and dependencies in AI-driven applications to ensure responsible and secure AI use.
CBOM	Software Bill of Materials for Cryptography	Lists cryptographic algorithms, keys, and certificates in software to ensure encryption standards and compliance. CBOM is also vital for Post-Quantum Cryptography (PQC) and quantum resiliency.
HBOM	Hardware Bill of Materials	Details physical hardware components to ensure a secure supply chain and device integrity by detecting counterfeit components.

The adoption of SBOMs, while still emerging in Canada, mostly happens in the telecom and financial sectors. It reflects a growing understanding of its role in supply chain resilience. Lessons from the U.S. and EU, where SBOMs are integral to cybersecurity strategies, further validate their importance and add them as pivotal building blocks in the companies' cybersecurity roadmaps.

Challenges in Implementing Software Supply Chain Security

Despite progress, Canadian organizations face hurdles in adopting robust supply chain security practices. Smaller organizations often lack the technical expertise or resources to implement standards and tools such as [SBOMs](#) and [VEX](#). The dynamic nature of software ecosystems, characterized by DevOps culture, continuous updates, and rapid development cycles, demands ongoing monitoring that many organizations find challenging to maintain. Additionally, the absence of universal standards for SBOM formats complicates integration across diverse environments. Addressing these challenges requires collaboration between government agencies, private-sector stakeholders, and international partners to develop scalable and interoperable solutions.

Recommendations for a Resilient Future

RECOMMENDATIONS FOR POLICYMAKERS

1. **Mandate SBOM Adoption:** Require the use of SBOMs across critical infrastructure sectors to enhance software transparency and ensure compliance with evolving cybersecurity regulations.
2. **Develop Incentives:** Provide financial or technical incentives, such as grants or tax credits, to encourage small and medium-sized enterprises (SMEs) to adopt supply chain security measures.
3. **Foster Global Collaboration:** Align Canadian policies with international frameworks like the NIST SSDF and EU Cyber Resilience Act to ensure interoperability and cross-border consistency.
4. **Strengthen Public-Private Partnerships:** Create intelligence-sharing mechanisms between government entities and private organizations to improve real-time threat detection and mitigation.
5. **Invest in Research and Development:** Fund initiatives to improve supply chain security technologies and methodologies, ensuring Canada remains at the forefront of innovation.

RECOMMENDATIONS FOR SMALL AND MEDIUM BUSINESSES (SMES)

1. **Start with SBOM Basics:** Utilize [open-source](#) or [commercial](#) tools to generate, ingest, and manage SBOMs, ensuring visibility into the software components used in your environment.
2. **Leverage Managed Security Services:** Partner with managed security service providers (MSSPs) to monitor supply chain risks if in-house expertise is limited.
3. **Educate Teams:** Train staff on basic cybersecurity hygiene, focusing on the risks of third-party dependencies and the importance of maintaining updated systems.
4. **Establish Incident Response Plans:** Develop plans to address potential supply chain breaches, including clear guidelines for engaging with vendors and customers.
5. **Adopt Scalable Solutions:** Implement lightweight, open-source security tools that fit within the budget and resource constraints of SMEs.

RECOMMENDATIONS FOR ENTERPRISES

1. **Integrate SBOMs into Asset Management:** Ensure all SBOMs are linked to enterprise-wide asset management systems for seamless tracking and vulnerability remediation.

2. **Conduct Supply Chain Audits:** Regularly assess the security posture of third-party vendors and enforce contractual obligations for cybersecurity compliance and SBOM sharing.
3. **Invest in Automation:** Use automated tools to continuously monitor software dependencies and detect vulnerabilities across the supply chain.
4. **Implement Zero Trust Principles:** Apply a zero-trust architecture to minimize the risk of lateral movement within your network in case of a breach.
5. **Collaborate with Policymakers:** Engage with government initiatives and frameworks to shape policies that address enterprise-specific challenges in supply chain security.

Emphasizing Education and Awareness

To mitigate risks, organizations must prioritize:

- **Training:** Educating teams on secure software development and supply chain risk management.
- **Awareness Campaigns:** Highlighting the risks of third-party dependencies and promoting a culture of vigilance across the technical R&D and operations teams.

Conclusion

Canada's evolving approach to software supply chain security, exemplified by Bill C-26 and CCCS guidance, positions the country along with the US and EU in addressing global cybersecurity challenges. However, continued focus on transparency, collaboration, and regulatory alignment is essential to mitigate the growing risks of supply chain attacks.

By adopting tools like SBOM management platforms, learning from global frameworks, and addressing implementation barriers, Canadian organizations can strengthen their defenses against increasingly sophisticated adversaries. As the software supply chain becomes a critical pillar of national security, proactive measures today will ensure resilience and the ability to respond and mitigate such threats for years to come.

For more information, refer to CCCS resources such as ITSM.10.071, [Common Criteria](#), and global standards like [NIST SP 800-218](#). ⁸

[Dmitry Raidman](#) is a Canadian-Israeli entrepreneur and cybersecurity expert with over 20 years of experience in application security, cloud architecture, DevOps, and cyber-defense automation. As co-founder and CTO of Cybeats, he has spearheaded innovations like the SBOM Studio and SBOM Consumer platforms that many Fortune 500 companies use to enhance their software supply chain management.



State of Cybersecurity in Canadian Retail

by [Isaac Wanzama](#)

The Canadian retail sector stands at the crossroads of digital innovation and heightened cybersecurity risks. [Employing over 2 million people](#) and contributing approximately 5% to the national GDP, the industry is critical to the economic fabric of the country. However, as retailers embrace advanced technologies like e-commerce platforms, AI-driven personalization, and contactless payments, they also expose themselves to increasingly sophisticated cyber threats.

In this report, Guardlii examines the state of cybersecurity in Canada's retail sector. Drawing insights from industry sources and our own ongoing survey of retail professionals, including executives, IT managers, cybersecurity specialists, and retail staff, we explore the financial, operational, and reputational impacts of cyber threats.

Additionally, we identify emerging trends and present actionable strategies for senior executives to address these challenges. By leveraging findings from this ongoing survey,

Guardlii captures diverse viewpoints across organizational levels, offering a nuanced understanding of cybersecurity priorities and challenges in the retail industry.

Table of Contents

1. Introduction
2. The Canadian Retail Landscape
3. Cybersecurity in Retail – Why It Matters
4. The Rising Cybersecurity Threats
5. Key Challenges in Canadian Retail Cybersecurity
6. Third-Party Vulnerabilities in Retail
7. Navigating Regulatory Compliance
8. Data Breaches and Their Cost
9. Strategic Solutions for Retail Cybersecurity
10. Final Thoughts

The Canadian Retail Landscape

Canada's retail sector is a diverse and dynamic contributor to the national economy. From global giants like Walmart Canada and Loblaw Companies Limited to innovative e-commerce platforms such as Shopify, the industry is a blend of tradition and innovation. Regional differences play a significant role in shaping the retail landscape. For example, urban centers like Toronto and Vancouver are hubs for high-tech retail experiences, while rural areas rely on localized supply chains and smaller retailers.

\$70B

is the approximate contribution the retail sector made to Canada's GDP in 2023.

The industry also supports over 2 million jobs, ranging from in-store personnel to logistics and IT professionals. Retail contributed approximately \$70 billion to Canada's GDP in 2023, underscoring its significance, according to the GDP by Industry Report 2023 by [Statistics Canada reports](#). This scale and complexity make the industry a prime target for cybercriminals, who exploit vulnerabilities at every level of the supply chain.

Cybersecurity in Retail – Why It Matters

The retail sector handles vast amounts of sensitive data, including payment information, personal customer details, and supply chain logistics. A breach in this data can lead to significant financial losses and harm customers' confidence. For C-level executives, the stakes are clear: cybersecurity is not just an IT issue; it's a critical business enabler.

Retailers face unique challenges due to the high volume of transactions and the integration of third-party systems. With the average cost of a data breach in Canada reaching \$7.05 million in 2022 by IBM Security, [The 2022 Cost of a](#)

Data Breach Report investing in robust cybersecurity measures is a strategic imperative.

The Rising Cybersecurity Threats

The retail sector remains one of the most targeted industries globally, with an estimated 10% of cyberattacks directed at retailers. Guardlii's survey confirms this trend, with 51% of respondents frequently encountering customer concerns about cybersecurity. Canadian businesses are no exception. Recent years have seen a rise in ransomware, phishing scams, and supply chain attacks, posing unprecedented challenges. Notably, the 2022 Sobeys ransomware attack disrupted operations nationwide, resulting in significant financial and reputational losses.

The shift to digital tools and processes in retail has created new opportunities for cybercriminals to exploit. Our survey found that 61% of respondents regularly check their systems for weaknesses, showing they are actively working to prevent risks. However, 16% of respondents admitted to never performing these critical checks, putting them at risk. The shift to e-commerce, coupled with increasing reliance on third-party vendors, introduces additional vulnerabilities. Guardlii's data highlights that enhancing third-party oversight is a top priority for many retailers, especially in maintaining compliance with frameworks like PCI DSS.

As retailers adopt advanced technologies like AI-based systems that identify threats and strategies that limit access to trusted users, their cybersecurity strategies must evolve to stay ahead of these threats. Guardlii's survey revealed that organizations investing in these innovations report significant improvements, such as increases in threat detection rates. However, 48% of respondents lacking cyber insurance underscores the critical need for financial risk mitigation alongside technological advancements.

Key Challenges in Canadian Retail Cybersecurity

The Canadian retail industry faces a unique and evolving set of cybersecurity challenges, shaped by the interplay of physical stores, e-commerce platforms, and third-party vendors. Insights from Guardlii's survey highlight critical areas that demand immediate and strategic action to mitigate risks and safeguard operations.

UNDERFUNDED IT DEPARTMENTS

For many retailers, particularly small to medium-sized businesses, thin profit margins constrain investment in cybersecurity. The survey revealed that 24% of respondents allocate less than 10% of their IT budgets to security,



limiting their ability to implement advanced tools and training programs. This lack of resources leaves many organizations vulnerable to increasingly sophisticated attacks and prevents them from addressing core weaknesses effectively.

LEGACY SYSTEMS

Outdated infrastructure continues to pose significant challenges for Canadian retailers. According to the survey, 20% of respondents struggle to integrate modern cybersecurity solutions with legacy systems. POS systems, which are critical for transactions, are especially at risk. Older POS systems often lack the encryption and security capabilities needed to defend against emerging threats like malware and API exploitation. These vulnerabilities make them a primary target for attackers.

REGULATORY COMPLEXITY

Canada's fragmented regulatory landscape adds another layer of difficulty for retailers. Navigating the differing requirements of provincial and federal laws, such as PIPEDA, while ensuring compliance with standards like PCI DSS, demands dedicated resources and expertise. For smaller retailers, the challenge of keeping up with these requirements can divert focus from broader security initiatives.

INSIDER THREATS

Employee actions—whether malicious or inadvertent—pose a significant risk to retailers, especially in an industry characterized by high turnover. The survey revealed that 31% of organizations do not provide employee cybersecurity training, leaving businesses exposed to insider threats and social engineering attacks. Building a culture of security awareness is essential to mitigating these risks and ensuring that employees serve as the first line of defense.

THIRD-PARTY RISKS

The retail industry's reliance on third-party vendors, from payment processors to logistics providers, introduces vulnerabilities that can compromise entire systems. While 50% of respondents rely on vendor risk assessments, many fall short in implementing continuous monitoring and contractual safeguards. Weaknesses in vendor security can lead to breaches that disrupt operations and damage customer trust.

Third-Party Vulnerabilities in Retail

Third-party vendors are integral to the retail supply chain, supporting operations from payment processing to logistics. However, these partnerships also introduce critical vulnerabilities. Insights from Guardlii's survey reveal that while 50% of respondents assess vendor cybersecurity through risk assessments, only 25% rely on compliance certifications, and 25% implement continuous monitoring. This highlights gaps in vendor oversight that could leave retailers exposed to cyber threats.

A weak link in a vendor's security can expose sensitive customer data or disrupt operations. For instance, phishing scams targeting vendor systems or ransomware attacks on logistics providers have previously halted deliveries and damaged customer trust. Guardlii's data emphasizes the need for proactive third-party risk management, especially as retailers increasingly rely on external providers for e-commerce and payment solutions.

To mitigate these risks, continuous monitoring systems are critical for identifying vulnerabilities in real-time. Additionally, clear cybersecurity standards in contracts, backed by regular audits, ensure vendors adhere to the retailer's security expectations. The

survey further highlighted the importance of adopting Zero-Trust principles, which help secure interactions between retailers and their vendors by enforcing strict access controls.

Navigating Regulatory Compliance

Compliance with regulations such as PIPEDA and GDPR is not just a legal requirement but a critical aspect of building trust with customers. These frameworks set standards for data protection and breach notification, ensuring accountability. For Canadian retailers, achieving SOC 2 compliance is particularly valuable, signaling a commitment to data security and often serving as a differentiator in competitive markets.

To navigate these regulations effectively, businesses should invest in training, leverage automation tools for compliance monitoring, and conduct regular audits. Compliance also builds consumer confidence.

Data Breaches and Their Cost

The cost of data breaches extends far beyond the immediate financial losses. Direct costs include fines, legal fees, and operational disruptions, while indirect costs encompass customer churn and reputational damage. The Sobeys ransomware attack of 2022 serves as a cautionary tale, illustrating how a single incident can ripple across the organization, halting operations and eroding trust. Investing in breach prevention and rapid response capabilities is critical to minimizing these impacts.

Strategic Solutions for Retail Cybersecurity

Effective cybersecurity strategies demand a multi-faceted approach that integrates advanced technologies, robust policies, and proactive training. Insights from Guardlii's survey of retail professionals reveal critical areas where these strategies can make the most impact.

A key approach is using advanced AI systems that analyze data to quickly detect and stop cyberattacks in real-time. Retailers adopting AI enhanced tools have reported improvements in detection rates, significantly reducing response times and minimizing potential damage. Survey respondents in IT management roles emphasized the importance of such tools in securing digital ecosystems.

Another important tactic is using strict security systems that verify each user's identity before granting access to any resource; "never trust, always verify." This approach secures networks by strictly enforcing authentication and

access controls. Interestingly, 31% of survey participants indicated that a lack of employee training on security protocols undermines these efforts, underscoring the need for integrated solutions.

Cyber insurance also plays a pivotal role, providing financial protection against the fallout from cyberattacks. However, the survey found that 48% of respondents lack cyber insurance, exposing their organizations to significant financial risks. Retailers that incorporate insurance alongside robust prevention measures position themselves for greater resilience.

Retailers that incorporate insurance alongside robust prevention measures position themselves for greater resilience.

Employee training emerged as a recurring theme in the survey, with 55% of organizations conducting monthly training sessions. This reflects a growing recognition of the role employees play in mitigating insider risks and reducing human errors. On the flip side, 31% of respondents admitted to never training employees, highlighting a critical gap.

Improving how companies monitor their external partners, like vendors, is another critical area highlighted in the survey. With many retailers relying on external vendors for supply chain and payment solutions, implementing contractual safeguards and deploying tools to monitor vendor compliance has become essential. Respondents flagged third-party vulnerabilities as a top concern, especially in maintaining PCI DSS compliance.

Finally, the survey emphasized the strategic importance of compliance. Many respondents noted that compliance is increasingly being viewed not just as a regulatory obligation but as a competitive advantage. Retailers that invest

in meeting and exceeding compliance standards can strengthen customer trust and bolster their market reputation.

Future Trends to Watch

Emerging technologies are reshaping the cybersecurity landscape. Blockchain works like a digital ledger, keeping transactions clear and secure, much like a bank statement, while quantum computing threatens to render traditional encryption obsolete [Deloitte's Cybersecurity Insights](#). Retailers must also prepare for adaptive compliance, as regulatory frameworks evolve to address new challenges.

Additionally, robotics is transforming the way stores operate. Innovations like automated checkouts and inventory management tools enhance efficiency but introduce unique cybersecurity risks, emphasizing the need for robust security protocols.

Staying ahead of these trends will require continuous investment in research and development.

Call to Action: Prioritizing Cybersecurity in the Canadian Retail Landscape

The Canadian retail industry faces unique challenges that demand strategic attention. High-profile incidents highlight the operational and reputational risks of inadequate defenses. Dependence on third-party vendors and fragmented federal and provincial regulations further complicate security efforts, requiring businesses to adopt tailored approaches to mitigate risks effectively.

Retail leaders must focus on building a strong security culture to protect their business and customers. Employees are often the first line of defense against cyber threats, yet many organizations lag in providing

adequate training. Implementing awareness programs can mitigate insider risks and reduce the likelihood of human error. Investments in modern technology are also essential for addressing vulnerabilities in legacy systems and adapting to evolving threats. Strengthening third-party oversight through contractual safeguards and continuous monitoring further protects supply chains.

Retailers that exceed baseline requirements can gain a competitive edge in today's privacy-conscious market. Additionally, collaboration with industry consortia, like CCN, cybersecurity firms, and government bodies provides access to advanced threat intelligence and innovative solutions, further enhancing resilience.

Cybersecurity must be central to every retail leader's strategy. By investing in people, technology, and partnerships, Canadian retailers can protect their customers, secure operations, and ensure long-term competitiveness in an increasingly digital marketplace. ⁸

Isaac Wanzama is the Founder of GuardlII Cyber Security Services, a firm specializing in safeguarding organizations against the rapidly evolving digital threats. With a proven track record as an accomplished entrepreneur Isaac is dedicated to empowering businesses, particularly within the retail sector—to strengthen their resilience against challenges such as ransomware, phishing attacks, and third-party vulnerabilities.





★★★★★
4.7 OUT OF 5



Overall Leader

MANAGED DETECTION
& RESPONSE

Take Your Cybersecurity Program to the **Next Level**

eSentire's all-in-one MDR solution combines cutting-edge open XDR technology, multi-signal threat intelligence, and 24/7 SOC-as-a-Service that delivers next level response, taking real action on your behalf to isolate 99%+ of threats at first host with a Mean Time to Contain of less than 15 minutes.

- ✓ **11x** Return on Investment on MDR Spend
- ✓ **Unlimited** Threat Hunting and Incident Handling
- ✓ **300+** Technology Integrations Supported

Protect your business with the G2 Overall Leader in MDR.

EXPERIENCE NEXT LEVEL MDR

eSENTIRE®



Safeguarding Canada's Power: Cybersecurity Landscape in Energy and Utilities

by [Denrich Sanada](#) and [Sonia Khan](#)

Executive Summary

The Canadian energy and utility sector is a critical pillar of the nation's economy and infrastructure, yet it faces growing cybersecurity threats driven by both financially motivated and state-sponsored actors. As reliance on digital systems increases and supply chain complexities intensify, cyber threats to operational technology (OT) and third-party vulnerabilities present heightened risks. This article provides an in-depth analysis of cybersecurity trends and threats in the Canadian energy and utility sector, underpinned by relevant statistics and strategic insights. With more than 75% of Canadian energy companies identifying supply chain risks as a primary cyber concern, proactive measures in cybersecurity have become essential. The piece

also addresses regulatory responses, organizational blind spots, and recommendations for resilience in a rapidly evolving threat landscape.

Introduction

As Canada embraces a transition to a digitalized energy grid, cybersecurity in the energy and utility sector has become a critical concern. The increase in interconnected systems has brought efficiency and resilience to energy distribution but also heightened the risk of cyberattacks. This article examines the state of cybersecurity in Canada's energy sector, highlighting current trends, emerging threats, and data on vulnerabilities impacting the landscape.

Trends Driving Cybersecurity in Canada's Energy Sector

1. Transition to Smart Grids and Renewable Energy

According to the Canada Energy Regulator (CER), Canada is aggressively pursuing renewable energy sources, with smart grids emerging as an essential component for managing these resources. Smart grids rely on data-driven insights to balance supply and demand across distributed energy sources, making them vulnerable to cyber threats targeting their operational technology (OT). The integration of renewable energy, however, also presents opportunities for cybersecurity, as distributed generation reduces the concentration of critical assets in single locations, dispersing risk.

2. Increasing Focus on Operational Technology (OT) Security

Cybersecurity for OT systems, which control physical processes like electricity distribution, has seen an increase in prioritization due to risks identified in the Cyber Centre's recent bulletin. Unlike IT systems, OT systems often operate with legacy infrastructure, which can be challenging to protect against advanced cyber threats. In 2024, the focus on protecting these systems is driving utility providers to allocate greater resources toward risk mitigation and endpoint protection within OT environments.

3. Investment in Artificial Intelligence (AI) and Predictive Analytics

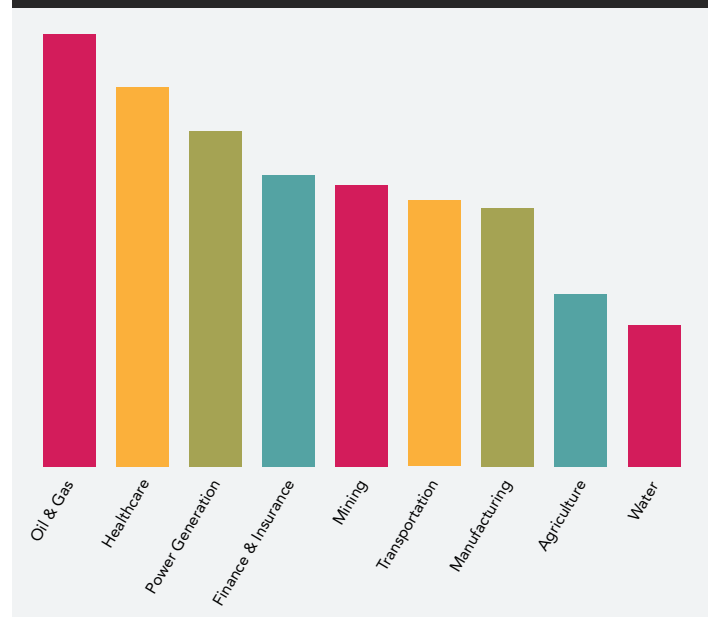
In response to growing threats, energy companies are increasingly investing in AI and machine learning to monitor for anomalies and predict potential attacks. These technologies, driven by data gathered across the network, enhance threat detection capabilities, allowing companies to respond before incidents escalate. This shift aligns with national cybersecurity objectives outlined in the National Cyber Threat Assessment 2025-2026, which highlights predictive analytics as a key tool for defending critical infrastructure.

4. Supply Chain Security

A noteworthy trend in cybersecurity is the increased scrutiny on third-party providers, as supply chain risks have escalated with the increased interconnectivity of systems. The interconnected nature of the energy supply chain necessitates thorough vendor assessments and adherence to rigorous cybersecurity standards, as breaches originating in supplier networks can compromise utility networks.

Key Cybersecurity Threats Facing Canada's Energy and Utility Sector

Percentage of critical infrastructure sectors in Canada reporting a cyber incident in 2019 Source: National Cyber Threat Assessment 2023-2024



1. Ransomware Attacks

Ransomware remains one of the most prevalent threats in the Canadian energy sector. As demonstrated by the recent cybersecurity incident at Suncor Energy, cybercriminals target energy companies for their critical role in national infrastructure, exploiting the high stakes to demand ransom payments. In Suncor's case, devices were swapped out after an attack to restore security. These incidents underscore the vulnerability of energy systems to ransom-based extortion tactics, which can disrupt service delivery and incur significant financial losses.

2. Insider Threats

Insider threats, whether unintentional or malicious, are particularly concerning in energy environments, where employees and contractors often have access to sensitive OT and IT systems. A Canadian Cyber Centre report highlights the importance of monitoring privileged access to prevent unauthorized actions that could compromise operational integrity. Enhancing insider threat detection through role-based access control and continuous monitoring has therefore become a standard practice in the industry.

3. State-Sponsored Attacks

State-sponsored cyberattacks pose a persistent risk due to the geopolitical importance of Canada's energy assets. The National Cyber Threat Assessment notes that state-sponsored actors, often aiming to cause disruption or gather intelligence, target critical infrastructure. These highly coordinated and sophisticated attacks can manipulate OT systems, making them difficult to detect and prevent. Their potential to impact national security necessitates collaboration between government and industry to safeguard critical assets.

4. Phishing and Social Engineering Attacks

Social engineering remains an effective tactic for attackers targeting the energy sector. The Canadian Cyber Security Centre's findings highlight phishing as a common initial access method for attackers, who then leverage compromised credentials to infiltrate networks. Utility providers are increasingly deploying training programs to educate employees on identifying phishing attempts, as awareness can be a crucial first line of defense.

5. Vulnerabilities in Industrial Control Systems (ICS)

ICS, which are essential to energy distribution, are especially susceptible to cyber threats due to their reliance on legacy technologies. The operational continuity of these systems makes them attractive targets, as disruptions can have severe consequences. Many Canadian energy companies are upgrading these systems or adopting new security measures, such as network segmentation, to contain breaches.

6. AI and Quantum Computing

AI, combined with quantum capabilities, may accelerate vulnerability discovery, enabling attackers to exploit

weaknesses rapidly. Quantum computing could break modern cryptographic ciphers, endangering encrypted communications, while AI-driven phishing and deepfakes could lead to more convincing disinformation campaigns and identity fraud. With AI relying on vast datasets and quantum computing offering unparalleled processing speeds, the risk of privacy breaches and identity theft grows, exposing sensitive information from seemingly innocuous data.

Key Data and Statistics

1. Distribution of Cyber Threat Types in the Canadian Energy Sector:

Ransomware attacks and phishing scams comprise 62% of cyber incidents reported by Canadian energy companies in recent years, making them primary attack vectors. Email fraud is a particular risk, with 77% of Canadian energy organizations reportedly lacking robust protections against these attacks.

2. Supply Chain and Third-Party Risk Perceptions:

According to PwC's survey, over 75% of energy and utility sector professionals in Canada view supply chain complexity as a significant risk to cybersecurity. Efforts such as enhanced third-party verification and cross-industry collaboration are emerging strategies, but blind spots remain in governance and accountability across supplier tiers.

3. Sector Spending on Cybersecurity:

Industry reports indicate that investments in cybersecurity have increased across the sector, with energy companies devoting approximately 10% of their IT budgets to cybersecurity in response to heightened threat levels and regulatory requirements.

4. Impact of State-Sponsored Cyber Activity:

Canada's National Cyber Threat Assessment highlights that geopolitical tensions have led to a surge in cyber espionage, with Canadian oil and gas companies identified as likely targets of state-sponsored cyber actors, who seek trade secrets and potentially exploit OT systems to disrupt operations.

5. Utility Cybersecurity Incidents:

Specific incidents, such as the recent cybersecurity breach at Suncor, reflect ongoing vulnerabilities. Suncor's response involved the replacement of hardware and an overhaul of cybersecurity protocols, underscoring the costly implications of such breaches on operational continuity.

Cybersecurity Measures and Resilience Strategies

1. Risk Management and Resilience Planning

Proactive risk management is now foundational in Canada's energy sector. Utility companies conduct thorough risk assessments that cover both IT and OT systems, enabling them to identify vulnerabilities and prioritize resources effectively. The sector's focus on resilience ensures rapid recovery in the event of an attack, with many companies implementing continuity plans and network segmentation to isolate compromised segments.

2. Implementation of Zero Trust Architecture

To combat insider threats, many energy organizations are adopting Zero Trust models, which require verification at every access point and limit lateral movement within networks. Zero Trust reduces the risk posed by compromised credentials, helping energy

companies prevent attackers from gaining access to critical systems even if they breach the network perimeter.

3. Enhanced Collaboration Between Industry and Government

To counter sophisticated threats, the Canadian energy sector relies on collaboration with government agencies, particularly through initiatives like the Canadian Cyber Threat Exchange (CCTX). Through such partnerships, energy companies share intelligence on threats and vulnerabilities, building a collective defense posture that benefits the entire sector.

4. Employee Training and Awareness Programs

Employee awareness is crucial in mitigating phishing and social engineering threats. Training programs tailored to the energy sector emphasize best practices for recognizing phishing emails and understanding the importance of cybersecurity hygiene. Companies also conduct regular simulations to test employee responses, reinforcing a culture of vigilance.

5. Adoption of AI and Machine Learning

Predictive analytics powered by AI plays a growing role in the energy sector's cybersecurity strategy. By analyzing vast amounts of network data, these technologies detect patterns that indicate potential attacks, allowing for timely responses. Such tools align with the national strategy to strengthen cyber defenses, as highlighted in the National Cyber Threat Assessment 2025-2026.

Conclusion

The Canadian energy and utility sector's growing reliance on digital technologies and interconnectivity requires heightened cybersecurity

measures to protect against evolving threats. Trends in AI, predictive analytics, and Zero Trust architecture, alongside a focus on OT security and supply chain resilience, equip Canada's energy sector to tackle a complex threat landscape. By adopting proactive risk management and fostering collaboration with government agencies, Canadian energy organizations are enhancing their cybersecurity posture, aiming to ensure a safe and resilient energy future. ⁸

References

[Canada's Energy Transition: Historical and Future Changes to Energy Systems – Update – An Energy Market Assessment](#)

[Suncor swaps out laptops after cybersecurity incident as energy sector takes stock of risks](#)

[National Cyber Threat Assessment 2025-2026](#)

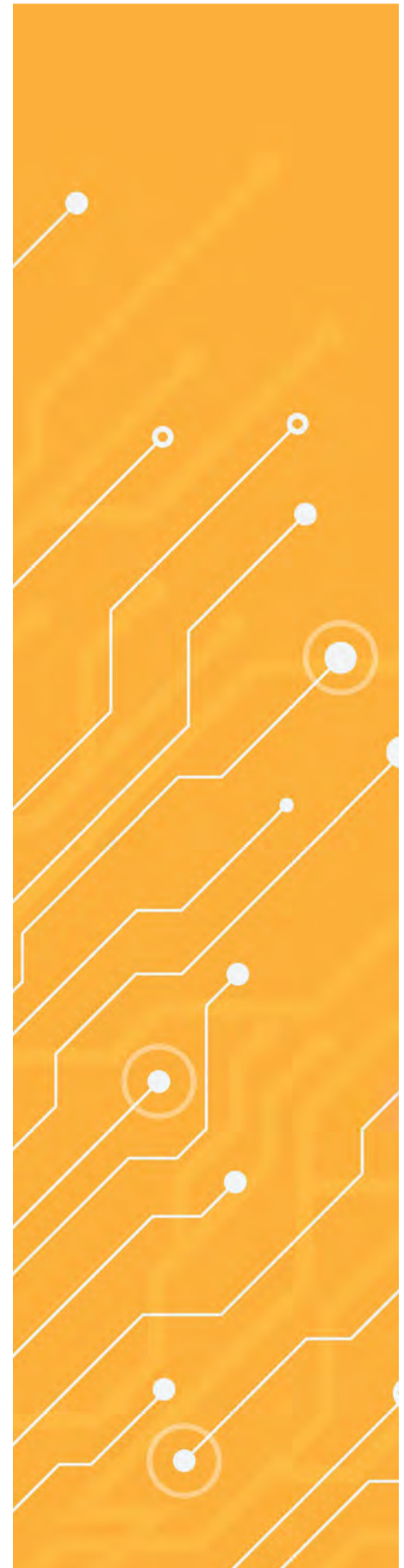
[Cyber threat bulletin: The cyber threat to Canada's electricity sector](#)

[News & Insights: Cybersecurity Threat Landscape in the Canadian Energy Industry](#)

[The top 6 trends shaping the energy sector in 2024](#)

Denrich Sananda is a seasoned Industrial Cybersecurity Consultant with extensive experience in securing Operational Technology (OT) environments. With a background in automation and a deep understanding of standards like NERC CIP, ISA/IEC 62443 etc., he specializes in assessing and mitigating cyber risks in critical infrastructure sectors across Canada and Middle East.

Sonia Khan is a Cybersecurity Consultant at Arista Cybersecurity Services, specializing in safeguarding critical infrastructure in Canada. With Master's in Electrical and Software Engineering, and years of experience in research and teaching, she focuses on developing secure, innovative solutions for the industrial and energy.





Beyond the Badge: Cybercrime Challenges and Solutions in Modern Policing

by [Lina Dabit](#)

Cybercrime investigations pose unique challenges for law enforcement globally. Many agencies established specialized units to combat computer-based in the early 2000s as the internet became widespread and cybercrime started to rise. As cybercrime continues to grow exponentially and threat actors capitalize on rapidly evolving technology, policing capabilities have not kept pace. Let's examine some of the significant challenges facing law enforcement today, but more importantly, the strategies being undertaken to effectively combat cybercrime.

The borderless nature of cybercrime means that jurisdictional issues continue to have an outsized impact on

investigations. Determining which country has the authority to investigate and prosecute complicates efforts to coordinate across borders. The collection of digital evidence, as well as the investigative processes utilized to collect it, can vary considerably. Additionally, legislative and legal frameworks vary by country which means that the definitions of cybercrime, and the relevant statutes, are not always consistent. Balancing the need for effective cybercrime investigations with the protection of individual privacy rights is an ongoing challenge. For example, a recent Canadian Supreme Court decision, *R v. Bykovets*, ruled that Canadians have a reasonable expectation of privacy

in their Internet Protocol (IP) addresses. As a result, law enforcement agencies must obtain judicial authorization to compel internet service providers to disclose IP address information. This ruling in particular is significantly more restrictive than many of our international partners and creates additional steps for Canadian law enforcement, which sometimes impacts how quickly information can be shared.

While digital investigations have been a part of criminal investigations for more than twenty-five years, they remain a highly specialized capability within policing. Police officers often have excellent investigative skills that allow them to apply their expertise to cases ranging from organized crime to homicides and global drug investigations. But many police officers do not have a tech background, and policing is ever more reliant on a small number of highly trained officers. Many law enforcement agencies struggle with limited budgets and resources while the development of effective cybercrime investigators takes a significant investment of both time and money. All while criminals rapidly change tactics to evade authorities and exploit the opportunities available in the cyber realm. One of the trends we are seeing is how cyber is fast becoming the underpinning of a significant component of criminality beyond ransomware; data and cryptocurrency cartels, money-laundering, organized crime trafficking in drugs, humans or data. If there is one thing I have learned in thirty years of policing, it is that criminals are adept at identifying and utilizing opportunities. The lucrative potential of cybercrime is seeing an emergence of “traditional” organized crime groups capitalizing on the reach and availability cyber represents. Yet policing continually takes a reactive rather than proactive approach, even while the pace of evolution in this space demands that we move more quickly to meet emerging threats.

The rapid evolution of technology presents both opportunities and challenges for law enforcement. As technology advances, cybercriminals develop increasingly sophisticated methods to commit crimes, and makes it harder for police to detect and respond to these threats. The emerge of AI in particular, can be a bane or boon depending on who you speak to. The reality is that AI is not one of the other; it is both, and can be leveraged for the power of good or bad. The difference is that law enforcement has a number of guardrails (rightfully so) to ensure that we operate within the confines of our legal authorities, while threat actors have ZERO rules.

One of the ways that AI in particular can be utilized effectively is to address the sheer volume of data law enforcement in Canada must contend with. Since 2016, Canadian

police have had to work under the constraints of a Supreme Court decision, *R v. Jordan* which established new rules for determining when a criminal trial is considered unreasonable. The Supreme Court set a presumptive ceiling of eighteen months for provincial court trial; this means that from the moment a charge is laid, police and prosecutors have eighteen months until the anticipated end of a trial. This is balanced against *R v. Stinchcombe*, another Supreme Court ruling that stipulates that the Crown must disclose all relevant information to the accused in a timely

Had our investigative team printed off all the evidence they gathered, the volume of paper would have filled an entire hockey arena.

and meaningful way. These rules are in place regardless of whether the crime is shoplifting or a major cyber-enabled fraud. The difference is that in the majority of cybercrime investigations, the volume of data is significant.

On our Netwalker affiliate investigation, had our investigative team printed off all the evidence they gathered, the volume of paper would have filled an entire hockey arena. In another investigation, more than eight (8) terabytes of data was seized and the significant resource draw to review and prepare the disclosure was considerable. As policing moves towards the use of AI and other cutting-edge technologies, I am confident this will greatly enhance both the timeliness and effectiveness of investigative responses of future investigations.

So how is law enforcement responding to these challenges? The collaborative approach to cybercrime is one of the most effective strategies we have in our arsenal. The willingness of international partnerships to share intelligence,

coordinate investigations, and work to apprehend cyber-criminals greatly mitigates the impacts of cross-border criminality. While Joint Force Operations (JFOs) are not new, the ways in which policing have come together to combat cybercrime demonstrates how effective we can be when we work together. Additionally, the emergence of public-private partnerships highlights a number of strategies that can be utilized in the protection of Canadians. The FBI recognized the value of public and private partnerships to combat cybercrime decades ago. Private sector entities have significantly more resources, both human and technology, than policing and their willingness to share these resources means that we are better equipped to combat threats to our critical infrastructure.

Many law enforcement agencies in Canada recognize the importance of building partnerships with private sector, academia and all levels of government. Both the National Coordination Centre (NC3) and the Canadian Centre for Cyber Security (CCCS) actively engage in public-private partnerships to enhance cybersecurity across Canada. These partnerships involve critical infrastructure owners and all levels of government to share threat information and strengthen Canada's resilience against cyber threats.

When I started policing thirty years ago, I never imagined a world where cybercrime was such a significant part of my work because it seemed more sci-fi than reality. But I am heartened to see how law enforcement has stepped up to the challenge and I look forward to seeing the evolution of policing in this space. @

Inspector [Lina Dabit](#) joined the RCMP in 1994 and started her career in BC working a variety of duties ranging from uniform patrol, drug section, major crime, intelligence, and border integrity.

After transferring to Ontario in 2008, she focused on organized crime, national security and established the RCMP interview team in Ontario. She was commissioned in 2017 as commander of the Toronto Air Marshals. Since 2021, she has led the Cybercrime Investigative Team with a strong focus on operational collaboration between federal, international and private sector partnerships.





Canada's Education Sector: A Low-Hanging Fruit for Cyber Criminals?

by [Lester Chng](#)

Why is the education sector at risk?

Canada's education sector – comprising K-12 schools, post-secondary institutions, and specialized vocational colleges – is highly reliant on technology for delivering and fulfilling key functions. The schools manage a vast amount of personal information and intellectual property. The population of end users of the organization's network and information systems also challenges the administration. The users range from students, contractors, industry partners, and staff. Building a security culture across a diverse population of users, especially where a large proportion are constantly changing, will continue to be a challenge for all educational institutions.

These are not unique challenges to the education sector.

However, some conditions make them a more enticing target for cybercriminals.

1. IT AND CYBERSECURITY INVESTMENT.

Corporations that manage large numbers of users and sensitive information tend to have the budget to support maintaining and upgrading technology. This is not the case for most educational institutions where lack of investments has hindered technology maintenance, adoption of security tools, and the manpower required to monitor and respond to cybersecurity alerts.

2. MONITORING ABILITY.

The lack of awareness of user behavior, indicators, or the ability to interpret data provides a challenge to detect and respond promptly. In a mature enterprise, tools are used to track user behavior, analyze patterns, and take precautionary action to alert security teams of anomalous actions. This is supported by policies for an employer to observe an employee's actions on a corporate machine legally. Both

technology limitations and policy constraints hamper the education sector.

3. CONTROL OF DIGITAL TOOLS.

The education sector has faced the onslaught of the artificial intelligence tools that the general population has rapidly adopted. Even if the IT teams have attempted to blacklist, educate, write policy, and enforce controls, it is likely students or staff have already misused these applications. The challenge remains for educational institutions to govern the adoption and appropriate use of digital tools.

4. PERSONAL INFORMATION AND INTELLECTUAL PROPERTY.

Educational institutions manage information that is highly valuable to cybercriminals. These range from personal information, health information, financial information, and intellectual property via research and collaboration with government and private sector organizations. There is also the risk that highly classified research or intellectual property can be stolen. The management and protection of information by classifying data, encryption, segregation of duties, access control and other means will fall short of enterprise industry standards due to the lack of resources and competing priorities.

5. LACK OF TRAINING AND PRIORITIZATION.

While most educational institutions have embarked on basic cybersecurity hygiene training, it is likely insufficient. The gap includes role-specific training for personnel with cybersecurity responsibilities. This gap affects everyone - from the IT team members struggling with new tools, new processes, and additional workload to leaders assigned cybersecurity responsibilities. The level of readiness required to respond to a significant cybersecurity incident adequately will take a concerted training regime and the support from leaders to prioritize resources.

What were the impacts of recent cyber attacks on the sector?

Cyberattacks on Canadian educational institutions produced a ripple effect of harm far beyond the immediate technical disruption.

1. OPERATIONAL DISRUPTIONS:

During significant cybersecurity incidents, such as ransomware, the educational process halts. Classes were suspended, assignments became inaccessible, and email services, school domains, internet services, and even phone systems

were offline. Lengthy recovery times hampered student learning outcomes and impacted institutional credibility.

2. FINANCIAL CONSEQUENCES:

The financial impact was multifaceted. Direct costs included forensic investigation, external IT support, hardware procurement, and legal fees. There were indirect costs, like damage to an institution's reputation and the subsequent loss of trust among current and prospective students.

3. DATA PRIVACY CONCERNS:

Breaches in educational contexts led to unauthorized access to highly sensitive information. This included student IDs, addresses, health records (if maintained by the institution), and financial information. In more severe cases, the institutions also lost information from vendors, staff, recruitment applicants, and special research projects. Privacy violations have long-term consequences, including identity theft risks for affected individuals and permanent damage to the institution's brand.

4. LEGAL AND REGULATORY RAMIFICATIONS:

Institutions that failed to protect their data adequately faced potential for legal consequences and risked running afoul of Canadian privacy laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and various provincial privacy statutes.

What does the future hold?

The threat actors remain active and constantly evolve their tradecraft and operating models, as reported by the Canadian Centre for Cyber Security in their [National Cyber Threat Assessment 2025-2026](#). While the collaboration of private and public sectors to disrupt key criminal organizations has yielded some promising results, cybersecurity threats will likely persist in the foreseeable future.

The education sector also faces a challenging backdrop. With high rising costs and other competing areas of concern, there continues to be a resource allocation issue that will hamper the technology upgrades and expertise needed to improve the cybersecurity posture of education institutions. Along with that, the recent policy changes impact the number of international students and exacerbate the problem as institutions are forced to tighten budgets.

The cyber risks remain high. The operating environment is far from ideal.

However, institutions cannot afford to remain passive.

What can be done?

Educational institutions need to continue the good fight. Those responsible for protecting these institutions must be resourceful, collaborative, and judicious in enhancing cyber resilience.

1. FOSTER A CULTURE OF CYBERSECURITY AWARENESS.

Building a robust cybersecurity culture is crucial. Institutions should prioritize ongoing training and awareness campaigns tailored to the diverse user base, including students, staff, and contractors. Cybersecurity hygiene cannot only be a checkbox exercise but a core component of the educational experience. Regular phishing simulations and interactive learning opportunities can reinforce good security practices.

Those responsible for protecting these institutions must be resourceful, collaborative, and judicious in enhancing cyber resilience.

2. LEVERAGE PARTNERSHIPS AND SHARED SERVICES.

Collaboration is essential for resource-constrained organizations. Educational institutions can pool resources by participating in shared cybersecurity services or collaborating with sector-specific organizations like the [Canadian Cyber Threat Exchange \(CCTX\)](#). Partnering with local government and private sector entities can provide access to expertise, tools, and threat intelligence that would otherwise be unaffordable.

3. ADOPT A RISK-BASED APPROACH TO CYBERSECURITY.

Institutions should identify their most critical assets—whether it's sensitive student data, research projects, or operational systems—and focus on securing these areas first. Implementing basic security measures, such as multi-factor authentication (MFA), network segmentation, and regular vulnerability assessments, can significantly reduce risks without requiring large investments.

4. INVEST IN INCIDENT RESPONSE PLANNING AND EXERCISES.

Preparation is the key to minimizing the impact of a cyber incident. Every institution should have a well-documented and regularly updated incident response plan (IRP). Beyond documentation, conducting tabletop exercises and simulated cyberattacks can prepare staff and leadership to respond swiftly and effectively when an incident occurs.

5. MAXIMIZE EXISTING TECHNOLOGY.

While budget constraints may limit the adoption of cutting-edge tools, institutions can maximize the use of their current technology by configuring systems correctly, applying patches promptly, and employing open-source or low-cost cybersecurity solutions where appropriate.

6. ADVOCATE FOR SECTOR-WIDE SUPPORT.

Education leaders must advocate for increased government funding and support for cybersecurity in the sector. Highlighting the potential long-term costs of inaction can help stakeholders understand the importance of proactive investment in cybersecurity measures.

Conclusion

Canada's education sector sits at a precarious crossroads. While it faces significant challenges, these challenges are not insurmountable. With strategic investments, cross-sector collaboration, and a steadfast commitment to fostering cyber resilience, educational institutions can protect their students, staff, and intellectual assets from the ever-present threats posed by cybercriminals.

You don't have to be at the top of the tree. Just don't be the lowest-hanging fruit. ☺

Lester Chng is a Senior Cybersecurity Advisor at the Rogers Cybersecure Catalyst, where he leverages his CISSP and PMP certifications to guide clients through complex cyber exercises and risk management initiatives. With extensive experience designing and implementing large-scale exercise programs across North America's financial services sector and within military environments, he is well-versed in navigating high-stakes, security-critical scenarios.



Addressing the talent gap: Focusing on mid-career transitions

by [Randy Purse](#)

The cybersecurity talent shortage continues to receive significant attention. And rightly so. A lack of cybersecurity talent creates additional risks for organizations and for Canadians writ large. For individuals and organizations, these risks translate to financial losses,

personal harms, and reputational damage in addition to other impacts. Beyond this, a lack of cybersecurity talent at the national level coupled with the increase in cybercrime and state sponsored activities, creates risks to our economy, our democracy, and our national security.

“70% of respondents agree that the cybersecurity skills shortage creates additional risks for their organizations... The most difficult roles to fill continue to be security operations and cloud security...54% of organizations say they struggle to recruit cybersecurity talent.” Based on a

global survey of 1850 senior IT and cybersecurity decision makers (Fortinet, 2024).

We should first define what we mean by cybersecurity talent in workforce terms. The majority of the attention is on the lack of cybersecurity professionals as defined by the [National Occupation Classification \(NOC\) 21220](#). We also need to keep in mind that there are many adjacent roles that require critical cybersecurity knowledge, skills, and abilities (KSAs) such as those in information technology, communications, engineering, software, business, and management. This latter group also warrants attention as they are a crucial component to addressing the talent gap. However, for this article, the focus will remain those we define as cybersecurity professionals where most of their work effort is on the application of KSA towards cybersecurity goals.

Dependency on post-secondary graduate to generate the workforce

Unfortunately, there is a paucity of reliable data on the cybersecurity talent gap or the available training and education in Canada. Based on current reporting on cybersecurity positions, we can see a shortage of between 10,000 and 25,000 in the coming years.

Post-secondary institutions are the traditional workforce generation channel. Based on the [Canadian Centre for Cybersecurity Post-secondary cyber security related programs guide](#), there are 144 Canadian cybersecurity courses and programs; this is over a two-fold increase since inception. Despite this, the talent gap has only widened as the demand across industry has increased.

That said, even if all (125) diploma, degree and certificate programs including advanced degrees produced a 30-person cohort every year, this would create approximately 3,750 workers assuming all graduated. This is, however, an optimistic estimate given the limited interest in cybersecurity programs, student attrition, and the increasing numbers of graduates leaving Canada for better opportunities.

If we are going to have a talent pipeline sufficient to address the need, we should be looking to better leverage alternative talent generation channels.

Another factor contributing to post-secondary educational challenges is that the quality of the programming is at times suspect. Employers are often frustrated by “gaps in practical training and a misalignment between academic programs and job readiness.” (CCN, 2024)

So, while Canadian post-secondary programming has significantly increased over the past decade, both its ability to generate sufficient job-ready graduates and its ability keep pace with the changing threat and technical landscape remain uncertain.

If we are going to have a talent pipeline sufficient to address the need, we should be looking to better leverage alternative talent generation channels. One channel that has shown tremendous promise is reskilling of the existing workforce.

Leveraging the existing workforce

“While organizations worldwide certainly face substantial challenges when it comes to safeguarding their digital assets, there are many strategies we can collectively pursue that will help to close the cybersecurity skills gap and augment individuals with the talent they need, and every organization needs. But recruiting and retaining qualified professionals will inevitably require creative strategies, and public and private sector organizations must collaborate to bring many of these to fruition.”
(World Economic Forum, 2023)

There is a large untapped pool of available talent – mid-career workers that are looking to transition to other careers. Presently, there are thousands of Canadian workers that are eager to transition to new careers. Many are in declining industries, are unemployed or feel underemployed. Others are simply looking at their potential futures and are seeking more sustainable work.

Broadly speaking, reskilling initiatives are intended to provide needs-based learning opportunities so individuals can obtain new or different KSAs that enable them to transition to and perform effectively in a new field of work. In cybersecurity, reskilling initiatives have demonstrated significant success at supporting over a thousand mid-career workers transition to cybersecurity work.

While delivered within different business and funding models, reskilling initiatives have some common characteristics:

- **They target specific workforce** gaps and provide rapid reskilling focused on industry needs.
- **Unlike most post-secondary programs**, they actively recruit into their programs including tapping into underemployed or underrepresented populations.
- **They will typically have an application** and screening process to help ensure that candidates are the right fit for the work.
- **They recognize the value of** experience and build on an individual’s existing competencies creating a far shorter learning pathway to proficiency.
- **They often include industry** recognized certifications or credentials that provide assessment and evidence of graduate competency for the work.
- **They typically have industry** sponsors or partners that help define the program, ensuring currency and relevance as well as providing work experience or employment opportunities for graduates.



- **They provide learning pathway** support using mentors or coaches that help guide the candidates through the program and connect the learning to their future work.
- **They provide career transition** support that assist candidates in identifying and preparing for the job search and, critically, getting employment in their new field.
- **Finally, the costs of the programs** may also be subsidized.

Examples of successful cybersecurity reskilling programs are provided in table 1.

Table 1 — Examples of effective reskilling programs

[Rogers Cybersecure Catalyst Accelerated Cybersecurity Training Program and Certifications for Leadership in Cybersecurity](#)

[Lighthouse Labs Cybersecurity Bootcamp](#)

[University of Ottawa’s Professional Development Institute, Coding for Veterans](#)


While not yet widely available or accessible across Canada, these programs have been quite successful at helping mid-career workers rapidly update their skills and transition to the cybersecurity field. A high percentage of the candidates fully complete their programs, obtain an industry relevant certification, and find employment within six months of completion. And based on reporting from the program operators, most graduates are that they chose a new career in cybersecurity; they have a future-proof career, potential for continuous learning and advancement, and garner well above average compensation and benefits.

Given the risks posed by the lack of cybersecurity talent, this seems to be a reasonable return on investment and a win-win-win for the workers, the employers and Canada. However, despite the growing need for cybersecurity talent, the success of these programs and the large untapped pool of mid-career workers, there is no sustained programming that is widely available.

Conclusion

“In Canada, we need to not only address the shortage (capacity) of cybersecurity talent, but also prepare for an expanding requirement and the evolution of the cybersecurity landscape (capability). Capacity means that Canada has the right number of people to meet the broader societal and industrial needs. Capability means that the people have the right competencies (knowledge, skills, abilities, and other characteristics) that can meet the need.”
(Technation, 2019)

While post-secondary institutions are helping to close Canada’s cybersecurity talent gap, they struggle to generate sufficient graduates to meet the industry needs of today and tomorrow. Continued investment in post-secondary institutions and



more agile approaches to curriculum design and program delivery will help ensure that they can produce more job-ready graduates.

In the meantime, however, the lack of cybersecurity talent means that we remain at risk. Reskilling programs have demonstrated the potential to:

- **Rapidly generate development** of cybersecurity professionals to help significantly reduce the cybersecurity talent gap;
- **Offer opportunities for thousands** of people in the existing workforce to pursue well-paid, sustaining careers; and
- **Provide a return on investment** at all levels through meaningfully employed, well-compensated workers, improved cybersecurity, and reduced risks with organizations and across the Canadian economy.

So, there appears to be a sound business case to invest in and expand reskilling programs for mid-career workers to help close the cybersecurity talent gap. Yet, these types of programs are not widely accessible across Canada and there appears to be limited commitment to their continuity in the face of several other competing priorities.

Understanding the risks that the cybersecurity talent gap presents to Canada and Canadians, this leaves one question: why aren't we considering a means to offer sustained, nation-wide delivery of these types of programs to more rapidly close the talent gap? ⁸

References

- Canadian Centre for Cyber Security (2024). [Post-secondary cyber security related programs guide](#), retrieved 18 October, 2024
- Canadian Cybersecurity Network (2024). [The cybersecurity skills crisis: Canada's call to action](#), retrieved 10 December, 2024
- Fortinet (2024). [2024 Cybersecurity skills gap: Global research report](#), retrieved November 8, 2024
- Technation (2019). Perspectives on a Canadian cybersecurity workforce development framework: A literature review.
- Statistics Canada (2021). [National Occupation Classification \(NOC\) 21220 Version 1.0](#), retrieved November 8, 2024
- World Economic Forum (2023). [How reskilling and upskilling talent can help shrink the cybersecurity skills gap](#), retrieved November 8, 2024
- Randy Purse, CD, PhD, CTDP is a veteran of the Royal Canadian Navy (RCN), with experience in several security roles, Randy is also the former Strategic Advisor of Cybersecurity Training and Education at the Canadian Centre for Cyber Security as well as the previous Director of Cybersecurity Standards and Vice President of Future Workforce Development at Technation. He joined the Rogers Cybersecure Catalyst at Toronto Metropolitan University in 2021 where he focuses on designing and facilitating cyber security training & education for a variety of academic and professional audiences. He continues to research, write and consult on cybersecurity, workforce development, and workplace learning.

Let us find you the best senior tech talent



“ We put Canada’s largest cybersecurity network to work for you and your company.”

François Guay

Founder of CCN and master recruiter

[Learn more](#)



Buggy Code: An In-Depth Look at the Cybersecurity Job Market

by [François Guay](#)

The cybersecurity job market is in a state of rapid evolution, driven by increasing demand for skilled professionals to address complex and ever-growing security challenges. However, much like a piece of buggy code that disrupts the functionality of a system, misalignments between job seeker qualifications and employer expectations are creating inefficiencies in Canada's cybersecurity workforce. This report synthesizes key insights gathered from job postings, employer surveys, and job seeker data to provide a comprehensive understanding of current trends, barriers, and opportunities.

Survey and Data Overview

The research encompassed a wide range of participants and methodologies to ensure a holistic perspective. Surveys targeted thousands of job seekers and hundreds of employers, utilizing online distribution and in-person small group discussions to gather detailed insights. Data on over 10,000 cybersecurity job postings from

[CanadianCybersecurityJobs.com](#), spanning three years, further enriched the analysis. This robust approach allowed for a nuanced understanding of the challenges faced by both employers and job seekers, revealing areas where alignment and strategic interventions are most needed — much like debugging a flawed system to improve overall performance.

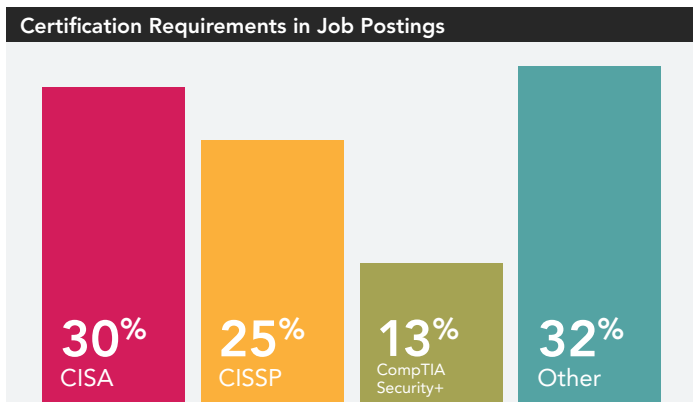
Canada's urban centers have assumed control of cybersecurity, leaving people from rural and smaller regional centers on the outside. In a country that depends on communications technology more than most due to its size, regional centers need to be producing cyber expertise because everywhere in Canada depends on ICT to connect, provide essential services, and participate in the digital economy. It is essential that we de-urbanize cybersecurity and move towards agile, smaller, regional programs that support both cyber awareness and expertise if all of Canada is to benefit from digital transformation.

— *Timothy King, ICTC*

Key Findings

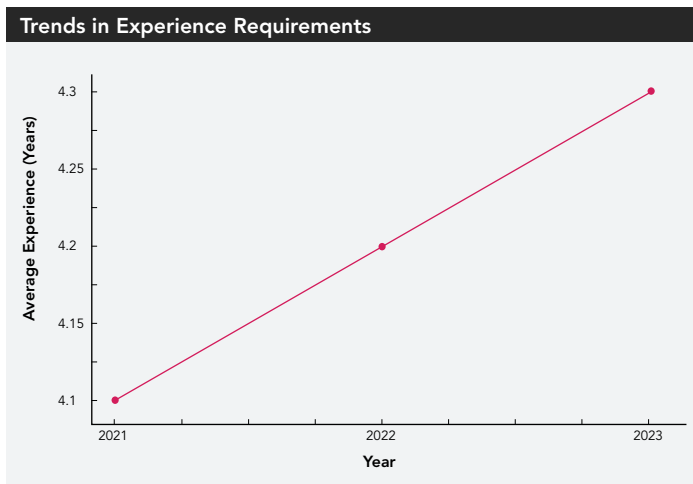
CERTIFICATIONS AND SKILLS

Certifications such as CISA, CISSP, and CompTIA Security+ were required in approximately 68% of job postings. Employers frequently highlighted deficiencies in certifications and technical abilities among candidates as major challenges, while job seekers expressed frustration with unclear pathways to certification and limited access to advanced technical training. This disconnect mirrors a scenario where buggy code causes breakdowns in communication between system components, leaving inefficiencies in the cybersecurity talent pipeline.



EXPERIENCE REQUIREMENTS

The average job posting demanded 4.3 years of experience, yet only 10% were entry-level roles. Employers cited long training cycles and misalignment between educational curricula and industry needs as concerns. Job seekers, on the other hand, identified the lack of entry-level opportunities as a key barrier to entering the workforce. Addressing this challenge is akin to debugging a program to ensure smoother interactions between inputs and outputs.



GEOGRAPHICAL CONCENTRATION

The majority of cybersecurity jobs were concentrated in Toronto (35%), Ottawa (22%), and Vancouver (15%). This regional focus creates accessibility challenges for candidates in other areas, while employers sought institutional partnerships to bridge gaps in underserved regions. Like buggy code, this geographical concentration limits functionality across the broader system — in this case, Canada’s workforce.



SOFT SKILLS AND DIVERSITY

Employers identified communication, teamwork, and diversity as critical gaps in the talent pool. Job seekers noted a lack of mentorship and industry promotion, which hindered the development of these vital professional skills. These gaps are reminiscent of missing modules in a program, leaving the system vulnerable and incomplete.

TECHNICAL SKILLS AND TOOLS

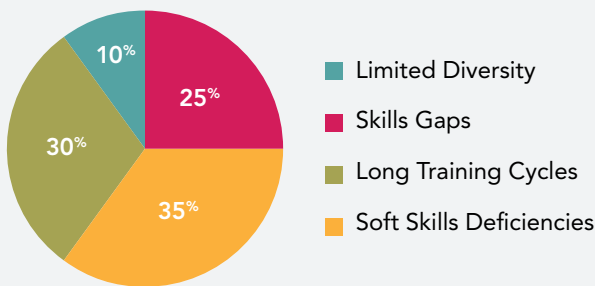
Skills in IAM, cloud security, SIEM platforms, penetration testing, and DevSecOps tools were in high demand. Employers emphasized the need for practical, hands-on training to reduce onboarding time, while job seekers felt their education was overly theoretical, lacking exposure to real-world tools. The lack of practical skills mirrors poorly tested code that fails to operate effectively in live environments.



Top Challenges Identified

- 1. For Employers:** Skills gaps, lengthy training cycles, limited diversity, and soft skills deficiencies.
- 2. For Job Seekers:** Scarcity of entry-level roles, high certification demands, and misalignment between education and practical job requirements.

Challenges Identified by Job Seekers



Recommendations

To bridge these gaps and debug the “buggy code” of Canada’s cybersecurity job market, the following strategies are proposed:

1. CREATE CLEAR CAREER PATHWAYS

Develop role-specific roadmaps with defined skills and certifications, supported by interactive guides for job seekers.

2. EXPAND AWARENESS CAMPAIGNS

Target underrepresented groups through outreach efforts, showcasing the diversity and scope of cybersecurity careers.

3. ENHANCE PRACTICAL TRAINING

Strengthen partnerships between academia and industry to embed hands-on experiences and apprenticeships into educational programs.

4. PROMOTE ENTRY-LEVEL OPPORTUNITIES

Collaborate with employers to create realistic entry-level roles and establish pipelines that combine training with hiring.

5. DIVERSITY AND REGIONAL ACCESSIBILITY

Advocate for remote work and decentralized job creation to reduce geographical barriers and increase inclusivity.

“‘Gone’ needs to be the days of ‘two years’ experience is required for entry-level positions. The path to national cyber-resilience may lie with a version of crowd-sourcing at scale — developing provincial and national programs that encourage or subsidize the apprenticeship and employment of entry-level staff to critical infrastructure and adjacent industries. With the threats currently noted nationally, the time is now.”

— James Cairns, Bow River College

Conclusion

The cybersecurity job market demonstrates a critical need for improved alignment between job seeker aspirations and employer expectations. Much like debugging faulty code, addressing gaps in certifications, practical training, and regional accessibility will require coordinated efforts between industry, academia, and government. By implementing the strategies outlined in this report, Canada can foster a robust, inclusive, and future-ready cybersecurity workforce — one that is free of the inefficiencies currently slowing its progress. ⁸

François Guay is the visionary founder of Canada’s largest cybersecurity network, the Canadian Cybersecurity Network (CCN), which unites over 44,000 members from diverse sectors, including individuals, businesses, universities, professional associations, diversity groups, and government agencies, representing nearly 1,000,000 people across the country. Under François’s leadership, CCN has become a cornerstone in fostering collaboration, innovation, and security in Canada’s rapidly evolving cybersecurity ecosystem.

Key Recommendations

Strengthening Canada's Cyber Resilience

The 2025 State of Cybersecurity Report underscores that a reactive approach to cyber threats is no longer sufficient. Organizations must transition to operational resiliency, ensuring they can continue critical functions even in the aftermath of a major cybersecurity attack. This involves implementing contingency plans that prioritize business continuity alongside robust cybersecurity measures. To fortify Canada's cybersecurity landscape, the report outlines the following actionable strategies:

1. ADOPT REAL-TIME CYBERSECURITY MEASURES

- **Prioritize advancements** like Identity Threat Detection and Response (ITDR) to address evolving identity-based threats. As Gartner highlights, ITDR is a cornerstone for managing risks in cloud and hybrid environments.
- **Implement continuous monitoring** systems to detect and respond to threats instantaneously, minimizing damage from attacks like ransomware.

2. ADDRESS THE TALENT GAP

- **Scale mid-career reskilling programs** to tap into underutilized talent pools, such as professionals from declining industries or underrepresented regions.
- **Expand regionalized training** initiatives to ensure equitable access to cybersecurity education across Canada. François Guay emphasizes, "We must de-urbanize cybersecurity to support a truly national digital economy."

3. STRENGTHEN PUBLIC-PRIVATE COLLABORATION

- **Create frameworks** similar to the U.S. Joint Cyber Defense Collaborative (JCDC) to align government resources with private-sector expertise.
- **Offer financial incentives** for SMBs to adopt Managed Detection and Response (MDR) services, enhancing their ability to detect and mitigate advanced threats.

4. FOSTER A SECURITY CULTURE

- **Invest in behavior-focused training** to address human error, which accounts for 82% of breaches according to a Verizon report.
- **Encourage leadership buy-in** to cultivate a cybersecurity-first mindset across organizations. Paul Da Silva aptly notes,

"Modern organizations can no longer rely on periodic snapshots or reactive measures. They need real-time, adaptive cybersecurity approaches."

5. HARNESS EMERGING TECHNOLOGIES

- **Embrace innovations** like AI-powered anomaly detection to enhance threat identification and mitigation.
- **Build frameworks** to manage risks associated with generative AI and deepfake technologies, which fraudsters are exploiting with increasing sophistication.

Conclusion

The findings and recommendations outlined in this report are a clarion call for stakeholders across Canada's cybersecurity ecosystem. By adopting real-time security measures, addressing the talent gap, fostering public-private collaboration, and cultivating a robust security culture, Canada can secure its digital future and maintain global competitiveness.

Organizations, educators, and policymakers must work in concert to ensure the strategies proposed here are implemented effectively. Together, we can create a more resilient and secure Canada, paving the way for sustained innovation and trust in our digital landscape. *With operational resiliency as the cornerstone of a robust cybersecurity posture, Canada can ensure that its critical systems remain functional, even under attack.* @

