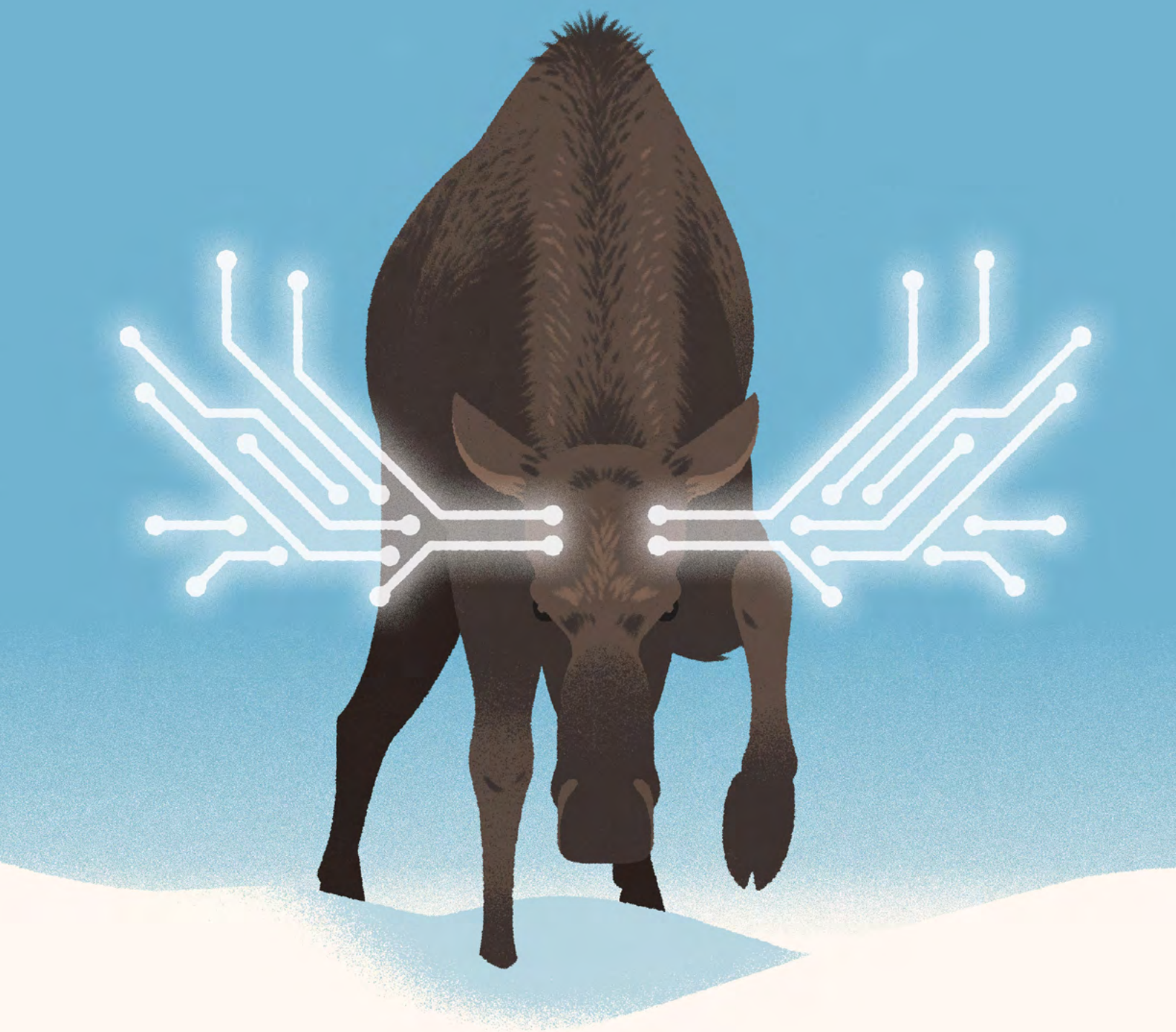
JAN. 2026

The State of Cybersecurity in Canada

PUBLISHED BY
Canadian Cybersecurity Network



TECHJUTSU DARKTRACE ccn

Table of Contents

Navigation Tips

Select page numbers in the table of contents to jump to corresponding articles.

Contributors

Matt Harrison Clough

Freelance Illustrator and the artist behind our cover

Amisha Parikh

Vice President of Security Solutions at Mastercard, Canada and author of *Strengthening Canada's Cyber Resilience: Key Insights and Recommendations*

Lina Dabit

Executive Director, office of the CISO at Optiv Canada and author of *The Human Factor of Risk: Understanding Insider Threats*

Navigation Tips

Select contributor head shots to jump to their articles.

Yellow underlined text indicates a link outside or within the report.

Tracey Nyholt

Founder and CEO of TechJutsu and author of *The New Face of Fraud: How Deepfakes Are Breaching Your Perimeter*

Jaap Mantel

VP of Sales at Data & More ApS and author of *Stop (Only) Securing the Perimeter: Your Data is Exposed, and You Don't Know Where to Look*

David Masson

VP, Field CISO at Darktrace and author of *Ten Insights into How AI Is Reshaping Cybersecurity in Canada*

Mary Carmichael

Managing Director of Risk Advisory at Momentum Technology and author of *How Leadership Decisions Make Cyber Breaches More Expensive*

Simon Hodgkinson

Advisor and Executive at Semperis and author of *Facilitating Cyber Crisis Tabletop Exercises: Insights from the Front Line of Simulation Leadership*

Munis Badar

Founder & CEO of Securetron and author of *Post-Quantum Cryptography (PQC): The Looming Cryptographic Shift*

Jonathan Weekes

President at BOXX Insurance and author of *Converging Paths: Where Cyber Insurance and Security Intersect*

Femi Ogunji

Senior Security Consultant and author of *2025: The Year Cybersecurity Became a Systemic Resilience Mandate*

Contributors

Cheryl Biswas

Independent Cybersecurity Analyst and author of *Securing Critical Infrastructure: Canada Can Light the Way Forward*

Scott Augenbaum

Founder of Cybersecure Mindset and author of *It Was Bad in 2018 — It's Worse Now*

James Cairns

Chief Information Security Officer at Bow Valley College and author of *Canada's Cyber Talent Pipeline Under Strain*

Navigation Tips

Select contributor head shots to jump to their articles.

Yellow underlined text indicates a link outside or within the report.

Michelle Balderson

Global Security Leader and author of *The Future of Cyber Leadership: The Rise of the Post Breach CISO*

Jason Keirstead

Cybersecurity Executive and author of *Model Egress: The New Security Perimeter No One Is Monitoring*

Evgeniy Kharam

Chief Technology Officer of Discern Security and author of *The Detection Gap: Why Security Controls Fail Before Alerts Fire*

Darwin Tusarma, Diego Ramirez and Rafael Ramirez

Authors of *Agentic AI and The Future of Canada's Security: A Nation at the Threshold of a New Digital Battlefield*

Richard Stiennon

Chief Research Analyst for IT-Harvest and author of *A Data Driven View: The Canadian Cybersecurity Landscape*

Jennifer Quaid

Executive Director of the Canadian Cyber Threat Exchange (CCTX) and author of *The Power of Collaboration*

François Guay

Founder of the Canadian Cybersecurity Network, Editor of *The State of Cybersecurity* and author of *The Global Race for Cybersecurity and Innovation*

Jen Spinner

Creative director of *The State of Cybersecurity*

Introduction

by François Guay

Canada enters 2026, at a defining moment for its digital future. Cybersecurity is no longer a specialized technical function operating quietly in the background. It has become a core pillar of national resilience, economic stability, democratic integrity and public trust. From AI powered fraud and identity manipulation, to ransomware supply chain disruption, foreign interference and quantum driven cryptographic uncertainty, the threat landscape has expanded in both scale and consequence. Yet Canada continues to demonstrate a quiet strength, grounded in collaboration talent and a steadily maturing cybersecurity ecosystem

The image on the cover of this report is intentional. The moose facing forward, grounded and alert is not a symbol of aggression but of resolve. It represents a country prepared to defend its space, its values and its digital sovereignty in the face of mounting conflict, complexity and constant probing.

Canada is not seeking confrontation, but it is no longer naïve to the realities of the modern threat environment.

Cyber risk today extends beyond systems and networks into identity trust cognition and financial and societal stability. Over the past year, the convergence of advanced technologies and human vulnerability has accelerated risk faster than most organizations can adapt.

Deepfakes, voice cloning and AI enabled social engineering now bypass traditional controls by exploiting trust rather than known technology. Identity has become the new perimeter and humans the most targeted attack surface. At the same time geopolitical instability, regulatory pressure and economic uncertainty, have elevated cyber resilience to a board level and national priority with consequences measured in operational disruption, financial loss and erosion of public confidence.

This report exists to provide clarity in that environment. The State of Cybersecurity in Canada 2026 examines where Canada stands today through evidence analysis and lived experience across sectors. It brings together insights from industry leaders, researchers, practitioners, insurers and former public sector and law enforcement officials to present a realistic view of risk readiness and resilience. Its scope, spans cybercrime and fraud identity and access management, AI and agentic systems, operational technology, cyber insurance crisis preparedness, quantum readiness and the strength of Canada's cybersecurity ecosystem.

The central argument is straightforward. Canada is resilient but uneven. Strong in talent innovation and collaboration, yet challenged by maturity gaps, fragmentation and rising identity based and human centered attacks. The question for 2026, is not whether threats will grow, but whether Canada can continue to strengthen its defensive posture, while preserving trust, accelerating innovation and protecting people, as much as infrastructure.

Executive Summary

Canada enters 2026 facing a cybersecurity environment defined less by isolated technical attacks, and more by sustained pressure on trust, identity, and resilience. Cyber risk has become systemic. Artificial intelligence enabled fraud, identity manipulation, ransomware, supply chain compromise, geopolitical interference, and the looming impact of quantum computing are converging to challenge not only organizations, but public confidence in digital systems. The question for Canadian leaders is no longer whether cyber incidents will occur, but whether institutions are prepared to withstand disruption, recover quickly, and preserve trust when they do.

The central finding of this report is that Canada is resilient, but uneven. The country benefits from strong talent, academic depth, a growing cybersecurity vendor ecosystem, and a collaborative culture across sectors. At the same time, material gaps persist in cyber maturity, particularly among small and mid sized organizations, legacy and operational technology environments, identity verification practices, and crisis readiness. Attackers are adapting faster than many organizations, and are increasingly bypassing technical controls by exploiting human trust through AI driven impersonation, deepfakes, and social engineering.

Identity has emerged as the new perimeter. Across finance, government, healthcare, and enterprise environments, attackers are targeting help desks, call centres, executives, and employees using highly convincing voice, video, and message based deception. Traditional signals such as caller ID, video presence, and voice recognition can no longer be relied upon. This shift renders purely technical defenses insufficient, and elevates the importance of zero trust identity verification, out of band authentication, and human centered security design. Organizations that continue to assume employees can reliably detect fraud on their own are increasingly exposed.

At the same time, the nature of cyber incidents has evolved from contained security events into full scale business crises. Ransomware and data extortion are now accompanied by regulatory pressure, media scrutiny, shareholder impact, and prolonged operational downtime. Despite widespread incident response planning, many organizations remain unprepared to execute under pressure. Tabletop exercises and crisis simulations reveal recurring weaknesses, including unclear decision authority, overreliance on technology assumptions, breakdowns in cross functional coordination, and lack of isolated communications capability. Preparation, rather than response quality, is now the decisive factor in resilience.

Cyber insurance has become a critical force shaping security outcomes. Insurers are no longer passive financial backstops, but active participants in prevention, setting baseline security expectations, and rewarding stronger hygiene. This convergence of insurance, security, and governance is raising the national floor of cyber practices, but also exposing maturity gaps, particularly among SMEs, where adoption of foundational controls remains low.

Looking ahead, Canada faces a second order transformation driven by agentic AI, and the transition to post quantum cryptography. Autonomous systems will accelerate both attack and defense, compressing decision timelines, and increasing the cost of delay. Quantum readiness is no longer theoretical, as harvested data today will be decrypted tomorrow. Crypto agility, asset discovery, and staged migration must begin now to avoid future systemic risk.

The overarching conclusion is clear. Canada is not falling behind, but it cannot rely on incremental improvement. Cyber resilience in 2026 demands a shift from perimeter defense to trust assurance, from reactive response to practiced readiness, and from siloed controls to ecosystem collaboration. The organizations that succeed will be those that treat cybersecurity not as a technology function, but as a leadership discipline anchored in preparation, identity, trust, and speed of response.

Strengthening Canada's Cyber Resilience: Key Insights and Recommendations

by Amisha Parikh, Vice President, Security Solutions, Mastercard, Canada

Canada's digital transformation has unlocked enormous opportunities, yet it has also escalated the risks we collectively face from increasingly sophisticated cyber threats. Mastercard's recent RiskRecon Report, analysing more than 4,900 organizations across 14 diverse sectors, offers a comprehensive view of our nation's cyber posture, emerging threats, and the steps leaders can take to build lasting resilience. Drawing on this research, here are the latest trends, solutions, and recommendations for enhancing cyber resiliency across Canada's interconnected digital economy.

Canada's Evolving Threat Landscape

The RiskRecon report identifies several national cybersecurity trends influencing today's risk environment. Although generally two-thirds of organizations received A or B cyber risk ratings (on an A-F scale), significant vulnerabilities persist, especially among small and mid-sized businesses, educational institutions, and manufacturers. This baseline performance is stable, yet the remaining one-third of organizations operating at C-F levels signal high-priority issues that can be addressed to reduce cyber risk exposures. Web based attacks, phishing and malware intrusions, dominate across sectors, exposing weaknesses in public-facing systems and gaps in cybersecurity policies. This highlights opportunities to adequately secure internal assets and the perimeter that faces the open internet.

Sector-specific vulnerabilities remain pronounced as well. Education and public service organizations, often operating under mandates requiring open and distributed IT environments, contend with a higher volume of critical cyber issues. The very nature of academic research and public data

stewardship, involving vast amounts of shared information, can inadvertently create broader exposure channels that malicious actors target frequently. Meanwhile, manufacturing and scientific organizations can face additional complex risks connected to the security of operational technologies (OT) and aging legacy IT stacks. These OT environments, often designed for longevity over security updates, can present a tempting target, as exploitation can lead directly to operational shutdowns rather than just data loss.

Noticeably, the use of unsupported or end-of-life (EOL) software in software services companies significantly magnifies breach risk, often in foundational web infrastructure. The report specifically notes concentrations of vulnerable PHP and Apache servers — software versions for which manufacturers no longer issue security patches, leaving systems exposed to known critical vulnerabilities. Furthermore, when examining infrastructure gaps, we see that open/exposed network configurations like unsecured MySQL servers create potential entry points for malicious actors. This underscores the importance of consistent, organization-wide risk analysis and auditing; many of these high-risk findings could be remediated with low efforts, minimizing high-risk exposures for entities.

Another accelerating trend is the surge in identity-related risk. Attacks involving credential theft, the creation of synthetic identities, and unauthorized account access have become increasingly prevalent, often fueling downstream ransomware and fraud schemes. Against this backdrop, robust identity verification systems and continuous monitoring emerge as critical top priorities for defense. Finally, the rapid development and accessibility of generative AI can amplify both defensive and offensive capabilities simultaneously. While defenders are beginning to employ AI for advanced threat detection and risk scoring, adversaries are increasingly leveraging these similar tools to automate reconnaissance, launch highly convincing, personalized scams, and escalate attacks with significant speed and scale, marking a potential distinct shift in the technological arms race.

Innovative Solutions

Meeting these evolving, technologically advanced challenges requires more than incremental improvements in standard controls; it demands collaborative and holistic solutions. Organizations across Canada are making impactful advances by embracing collaborative models that integrate cross-sector partnerships and specialized internal methodologies, such as cyber fusion models. At Mastercard, we see first-hand how essential B2B investments in cybersecurity may translate into tangible benefits for Canadian business owners and consumers. When financial institutions, merchants, and technology partners unite to strengthen digital payment infrastructure and support the digital landscape with information-sharing protocols, consumers can gain increased protection from fraud, identity theft, and data breaches that impact their personal finances.

> The traditional separation between fraud, cybersecurity, and compliance teams is increasingly dissolving in favour of integrated cyber fusion models.

Innovation is also transforming how internal teams operate. The traditional separation between fraud, cybersecurity, and compliance teams is increasingly dissolving in favour of integrated cyber fusion models. These models may speed up detection and response by breaking down internal silos and enabling multidisciplinary collaboration when an incident occurs. This integration appears crucial because modern fraud increasingly relies on compromises in cyber infrastructure and unauthorized access to data and systems. Across Canada, many organizations are turning to AI-powered solutions to help amplify their efforts against these complex threats. These next-generation tools are designed to drive faster, more accurate threat detection, integrate with identity verification platforms to validate access claims, and help organizations prioritize incidents based on meaningful business impact, helping security and fraud teams act decisively across a rapidly changing landscape.

The Path Forward: Building a Resilient Ecosystem

Looking ahead, enduring cyber resilience in Canada rests on a clear, strong commitment to action. Organizations should anchor their defense in strong, proactive cyber hygiene, including continuous risk assessments, comprehensive patch management across all domains (IT and OT), and foundational security controls that are validated regularly. Special attention should be paid to retiring or

strictly segmenting end-of-life systems to help ensure that known, high-severity vulnerabilities are not left exposed indefinitely.

Supporting small and medium enterprises remains a national priority. These organizations are economic cornerstones but frequently lack the budget or dedicated personnel for robust cyber infrastructure, leaving them disproportionately at risk. Expanding their access to proven, pragmatic tools and accessible guidance will help lift the collective baseline of defense for the entire digital supply chain. Meanwhile, ongoing education for staff, partners, and customers remains crucial, especially as scams and social engineering tactics become increasingly sophisticated due to cyber criminals and fraudsters leveraging generative AI tools to write perfect phishing emails or develop realistic deepfake videos.

To combat identity-centric attacks, renewed focus should be placed on modern, adaptive identity verification solutions deployed across all touch points. Organizations can proactively join and participate in sector-specific coalitions, leveraging shared threat intelligence to accelerate learning and the adoption of industry-wide best practices. Lastly, the responsible adoption and effective integration of AI-powered security tools, balanced with human oversight, could be the defining factor in whether organizations can stay ahead of increasingly automated adversaries in the years to come.

Canadian organizations have made tremendous strides in strengthening their security posture in recent years. Yet, the persistence of web-based attacks, scams leveraging coalition messaging, legacy technology vulnerabilities, burgeoning identity fraud, and the dual-edged capabilities of AI mean that a united, ecosystem-focused approach may prove critical. With cross-sector collaboration, ongoing investment in advanced tools, and an unwavering commitment to digital trust, Canada is well-positioned to navigate future cyber, identity and fraud risk and continue advancing in digital resilience.

Recommendations for Canadian Leaders

1. Conduct regular risk assessments, comprehensive patch management, and deploy foundational security controls.
2. Expand access to practical resources and support, as small and medium enterprises often lack robust cyber infrastructure.
3. Decommission or segment EOL systems, with rigorous monitoring and controls when retirement is not possible.
4. Deliver ongoing education for staff, partners, and consumers, leveraging the latest intelligence and coalition messaging.
5. Share information, tools, and best practices through coalitions and consortia for mutual defense.
6. Deploy advanced, adaptive solutions to combat new forms of digital identity fraud.
7. Integrate AI and automation across fraud detection, threat monitoring, and response strategies.

This article leverages Mastercard's RiskRecon Report: Risk Posture Analysis Canada (2025).

As the Vice President of Security Solutions at Mastercard in Canada, Amisha Parikh plays a leading role in strategy development to help drive payment innovation, security and resiliency.

Mastercard remains committed to strengthening the digital ecosystem through advanced fraud prevention, data-driven insights, and close collaboration with partners — helping ensure digital commerce is safe, seamless, and trusted.

Canadian organizations face invisible cyber risk. **See it before it strikes.**

Mastercard's RiskRecon analysis uncovers where Canadian industries are most exposed — from external vulnerabilities to supply-chain blind spots. Equip your organization with the visibility needed to stay secure.

Explore the report

cybersecurity & fraud prevention for enterprise

The Human Factor of Risk: Understanding Insider Threats

by Lina Dabit

What do Marks & Spencer, Coinbase, and Jaguar Land Rover have in common? They all recently suffered significant impacts as a result of an insider breach. Insider threats are nothing new. In fact, we've seen numerous instances woven throughout history; from the plunder of burials in ancient Egypt by grave robbers with inside knowledge of tombs to thefts from merchants and trading companies in the 17th and 18th centuries by employees with privileged access.

The risks posed by insider threats are so much more complex than the result of a disgruntled employee seeking revenge or monetary gain. Today's threats must be viewed as a spectrum ranging from unintentional, malicious, coerced and compromised. More importantly, we must understand how the lines between these risks have blurred, and how we can strengthen defences to detect, prevent and respond.

The Evolving Landscape

In our hyperconnected world, insider threats have evolved beyond human actors. What once was a uniquely human-centric risk has expanded to a broader challenge shaped by the growing use of non-human identities and autonomous agents. A recent conservative estimate puts the ratio of machine identities to humans at 82:1 in organizations worldwide. While this sub-category of insider threats warrants an entire article (or two) on its own, the

reality is that the majority of breaches currently have people as the vector. Additionally, 90% of security professionals will tell you that insider threats are more difficult to detect, taking an average of 86 days to contain while carrying significantly higher costs than a typical external attack.

Organizations have historically built cyber defence around the perimeter with the assumption that threats are from the outside. But the shift to cloud and remote/hybrid work along with complex supply chains and an increasing volume of third-party vendors have changed how we view the perimeter with the real danger increasingly within our walls.

As cybersecurity trends evolve, so do the risks around insiders with several prevalent threats increasingly front and center for many organizations:

- The explosion of AI and the ease of use by all employees regardless of technical expertise and knowledge of security protocols has seen a corresponding increase of associated risks. Shadow AI has led to the loss of intellectual property, compliance and regulatory violations, security vulnerabilities in unvetted/unapproved AI tools and data leakage.
- Third party and supply chain compromise continue to adversely impact organizations from small and medium-sized businesses to industry giants like Jaguar Land Rover. The complexity and interdependence of the supply chain backbone of daily operations means that these critical links are also the most vulnerable to cyber threats. Recent data suggests that roughly 30–35% of all breaches trace back to third-party or supply chain weaknesses, with supply chain attacks rising 42% in 2024 alone. The old saying "the chain is only as strong as the weakest link" is more relevant than ever. A single supplier with lax defenses can become a superhighway for attacks targeting other enterprises.
- Insider threats are blurring with external actors and increasing risks for organizations facing both trusted-access misuse and external adversary tactics simultaneously. Organizations are increasingly facing scenarios where employees can be coerced or deceived into providing access to external threat actors.

Insider Risk Threat profiles

Next we explore the key profiles that shape insider risk today.

MALICIOUS AND COERCED INSIDERS

Common profiles that jump to mind when we think of malicious insiders include:

- A disgruntled employee
- An employee who joins a company with the intention of stealing intellectual property or valuable information
- An employee who suddenly finds themselves in financial straits

While these types of insiders account for approximately 25% of insider incidents, their costs are disproportionately higher, especially when they target sensitive data, intellectual property, or critical infrastructure.

A malicious insider is any employee, contractor, or trusted individual within an organization who intentionally misuses their access, but a coerced insider is a legitimate user who is forced or pressured into abusing their access. From an intent perspective, this is involuntary, and these employees knowingly participate under duress,

forced to misuse their access or hand over credentials.

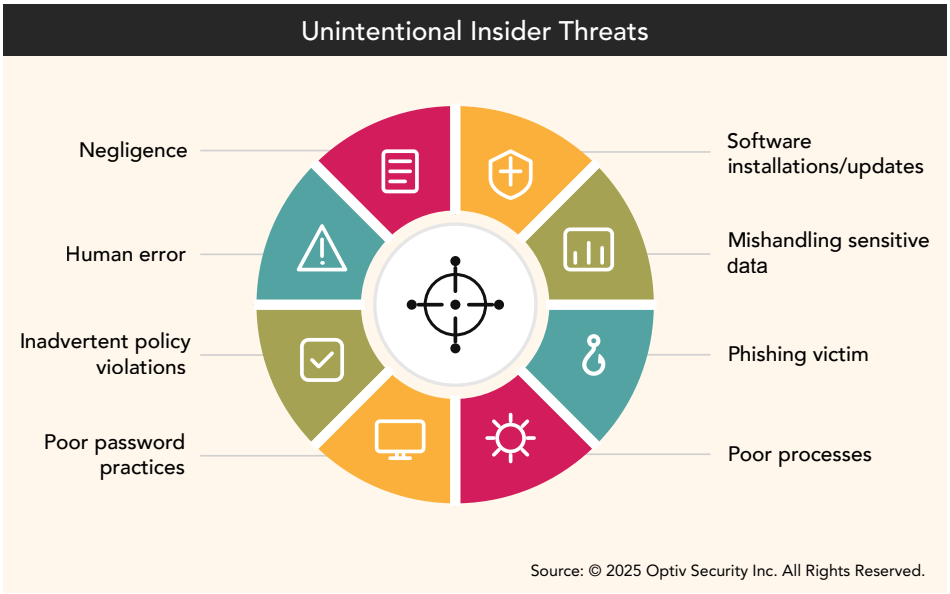
There are several ways that threat actors have been effectively leveraging pressure at both the organizational level, and increasingly, at the personal level.

This exploitation includes the utilization of threats against employees and their families, doxxing, blackmail, and the use of honeypots to manipulate employees into compromising scenarios to maximize power over them.

UNINTENTIONAL INSIDERS

While malicious insiders have an oversized impact on organizations, unintentional insiders continue to account for the largest proportion of risks with approximately 68% of breaches involving a non-malicious human element. This includes common vectors like phishing, human error, and negligence.

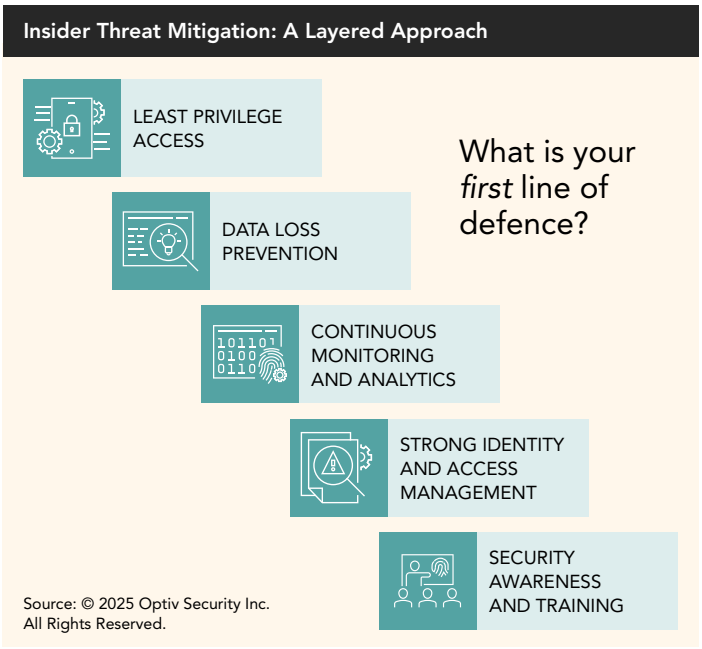
In some instances, poor enterprise policies and processes themselves contribute



to an increased threat landscape. For example, I was recently speaking with a client who shared that their approach to mitigating risks was a zero AI policy on all company devices. However, when I spoke to the employees about utilizing AI, they shared that when they needed to capitalize on how AI could improve their workflow, they simply input company information into their personal devices because AI on their work devices was strictly forbidden. The very policy that was implemented to mitigate risk, ended up being the very driver of risk. The organization not only lost control, but they also lost visibility into how and where their sensitive data was shared.

MITIGATING INSIDER THREATS

There is no simple solution for mitigating insider threats and technology alone cannot fix a human issue. However, a layered approach that combines technology, HR, and security awareness gives organizations the best opportunities to detect and respond early.



That said, the first line of defence is the human firewall. When employees feel supported and know what to do, they become part of the solution, and risks are contained and mitigated sooner. Fostering a positive culture needs to be an authentic approach that highlights how cybersecurity awareness and training starts at the top.

Finally, organizations should ask themselves if employees feel empowered to speak up if they are approached, threatened, or witness anomalies within their environments. Is the current security culture punitive? Are employees afraid to speak up? Is training framed as a remedial directive and punishment that singles out employees, or is it presented as a learning opportunity to enhance the organization?

When done right, security culture can transform cybersecurity from a purely technical function into a shared organizational mindset that strengthens employees individually and as a team.

Lina Dabit has three decades of law enforcement leadership spanning frontline policing to national security, major and organized crime, protective operations and cybercrime. She has built and led teams tackling complex threats, both physical and digital, and worked at the intersection of intelligence, technology, and public safety. Now stepping into the role of Executive Director, office of the CISO at Optiv Canada, Lina brings a mission-driven approach to cybersecurity; combining operational insight with a passion for innovation and resilience.

The New Face of Fraud: How Deepfakes Are Breaching Your Perimeter

by Tracey Nyholt, Presented by TechJutsu

The Next Frontier of Social Engineering

Security professionals have spent the last decade hardening perimeters against phishing emails and credential stuffing. We have deployed firewalls, endpoint protection, and robust Multi-Factor Authentication (MFA) to lock down access. Attackers have been equally busy finding new ways around these defenses, and they are using the trust you have in your own employees against you.

That trust is being systematically exploited by impersonation, spoofing and social engineering with voice AI at a growing scale. The rise of generative AI has brought with it a dangerous new threat of advanced deepfakes that are increasingly available to the general public. These are much less clumsy than the cute but uncanny versions from the past. Today's audio deepfake technology can clone a CEO's voice with just a three-second audio sample. Video deepfakes are becoming no less impressive, able to generate real-time overlays of a subject, making that face on the other side of a Zoom call much less trustworthy.

With the breathtaking speed at which these technologies are developing, a growing security gap is becoming critical. When your employees can no longer trust what they see or hear, the traditional "human firewall" begins to crumble.

The financial sector has already seen the devastating potential of this technology. A finance worker at a multinational firm based in Hong Kong was tricked into

transferring $25 million in 2024. This worker was instructed to do so on a video conference call. The call appeared to be populated by the company's CFO and other colleagues, but almost everyone on that call was a deepfake persona generated in real-time (CNN 2024). This incident dispelled the notion that video presence equals proof of identity.

Voice cloning has added a dangerous new tool to vishing (voice phishing) scams. In one high-profile case, attackers used an AI clone of the CEO of a UK-based energy firm. They were able to successfully direct the transfer of €220,000 to a fraudulent supplier (WSJ 2019). By replicating the specific cadence and tone of a company's leadership, fraudsters can bypass the skepticism that would normally stop a suspicious call or email.

Emerging biometric hacking tools are making it increasingly difficult for organizations to distinguish between legitimate users and impostors.

These are not isolated events. The FBI's Internet Crime Complaint Center (IC3) has warned that emerging biometric hacking tools are making it increasingly difficult for organizations to distinguish between legitimate users and impostors (FBI 2023).

Most organizations still rely on sensory confirmation for sensitive requests. If we see a face on a webcam or hear a known voice on the phone, our brain defaults to trust. Deepfakes exploit this biological vulnerability. Traditional signals like caller ID and voice familiarity are no longer reliable.

Current verification methods are ill-equipped to handle this:

- **Video Calls:** Standard video conferencing tools do not natively verify that the video feed is authentic and not a synthetic overlay.
- **Voice Recognition:** As noted by the Federal Trade Commission, scammers can now clone voices for as little as a few dollars, rendering voice recognition software increasingly unreliable for high-security authentication (FTC 2023).
- **Knowledge-Based Verification:** Asking "security questions" is futile when the attacker has likely already scraped the answers from LinkedIn or the dark web.

We can no longer assume that your employees will be able to identify fraudulent callers. Technology is evolving faster than human perception, and it is a race we are destined to lose.

To put a stop to this new wave of AI-powered fraud, we must move beyond reliance on audio/visual cues and implement verifiable trust. We need to treat a video call or a phone request with the same "zero trust" scrutiny we apply to a network login attempt.

Organizations must rethink identity for the voice channel as a first-class security problem. Beyond a simple customer service utility, calls into your service desk are becoming a critical attack surface operating on an outdated model of implied trust. Telephones are the path of least resistance for attackers struggling with firewalls and endpoint protection. Phone-based requests for password changes or MFA resets must be considered on the same security tier as network access requests.

LEVERAGE OUT-OF-BAND AUTHENTICATION

NIST Digital Identity Guidelines (SP 800-63B) recommend the use of out-of-band (OOB) authenticators (NIST 2025). Using something outside of the voice or video call to authenticate a caller effectively eliminates the human factor that attackers are relying on with their deepfakes.

Tools that push a secure MFA challenge to the user's registered computer or mobile phone during a call can provide assurance that the caller is who they claim to be.

HARDEN THE HELP DESK

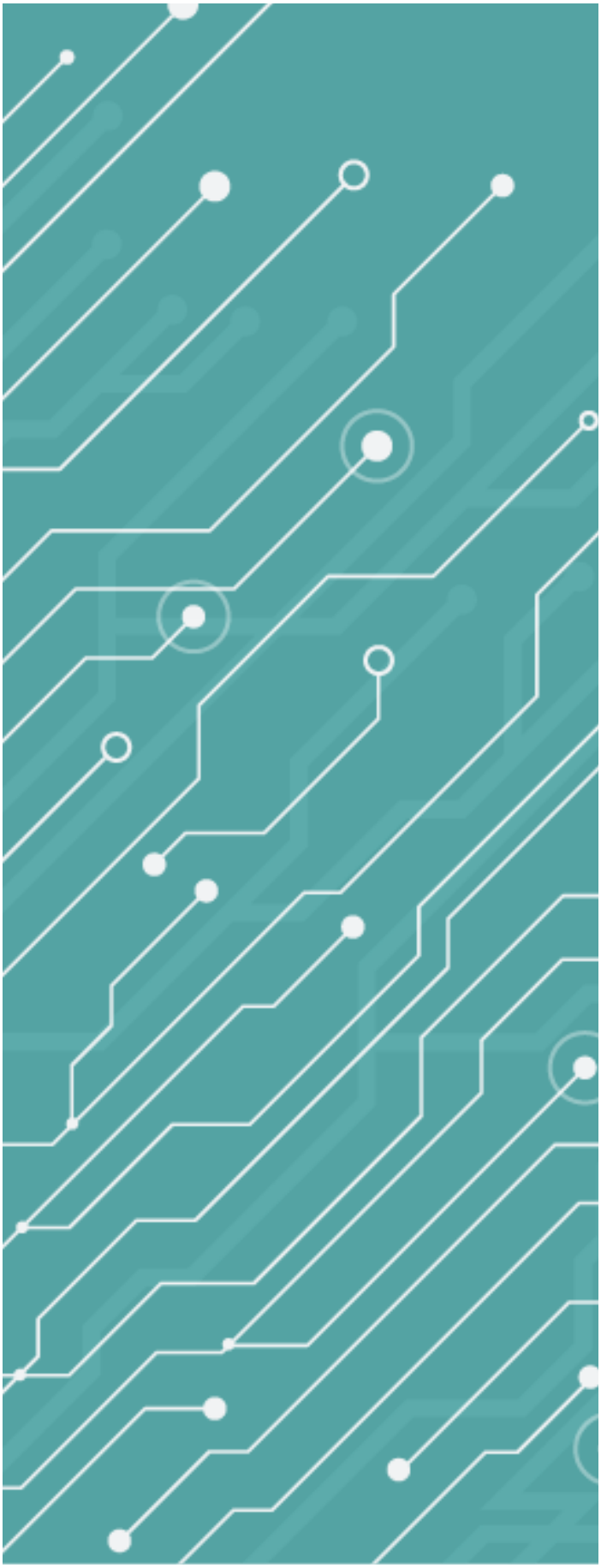
Integrate identity verification directly into your ITSM platform and call processes. Ensure that sensitive operations require secure user verification prior to making those changes.

Rather than rely on antiquated methods like easily guessed security questions, mandate that agents use phishing-resistant factors to authenticate callers. Empowering your service desk agents with tools that validate identities, you can ensure that they continue to both help and protect your organization.

By integrating robust, out-of-band authentication into our communication channels, we can inoculate our organizations against this new breed of fraud without crippling our operations. The technology to fake a face or clone a voice is here and becoming increasingly simple for even casual attackers to leverage. The counter-measures we deploy must not be cumbersome, however. We must ensure that digital identities are rigorously protected while simultaneously guaranteeing that the user experience remains as frictionless as possible. Security controls that frustrate users are security controls that are bypassed at every opportunity. Therefore, the goal is not just to build a higher wall, but to build a smarter gate. A gate that leverages the seamless, one-tap verification methods that employees already use in their everyday lives to deliver rigorous identity assurance in seconds. By balancing unyielding cryptographic security with intuitive, user-centric design, we can restore trust to our conversations without sacrificing the speed of business.

See end notes for this article's references.

Tracey Nyholt is the founder and CEO of TechJutsu, an IAM and cybersecurity firm specializing in closing security gaps in help desks and call centers. TechJutsu's Caller Verify solution allows call center agents to securely verify a caller's identity with the caller's own MFA factors.



TRUST IS A TWO-WAY ROAD

Secure the full circle of communication

BUILT FOR REAL ATTACK SCENARIOS

Eliminate social engineering risks by stopping impersonation attempts

REAL-TIME CALLER VERIFICATION

Verify every caller in under 10 seconds using secure MFA

RAPID DEPLOYMENT

Go live in as little as one day with seamless ITSM integrations

Canadian-built cyber solutions

www.callerverify.com

Stop (Only) Securing the Perimeter: Your Data is Exposed, and You Don't Know Where to Look

by Jaap Mantel

Large software providers have spent the last quarter-century promoting the promise of centralized data management and integrated processes. Despite massive investment, this vision remains largely aspirational. This paper shifts the focus from vendor promises to organizational reality.

We will examine the core challenges and critical considerations organizations face in establishing a functional, reliable foundation for Governance, Risk and Compliance (GRC), Security, and Artificial Intelligence (AI) strategy, all anchored in accurate data classification. While the industry echo chamber bombards us with messages of digital transformation and revolutionary technology, a fundamental gap persists: Data Blindness.

The most significant challenges contributing to this gap are:

- **Ineffective Governance:** Organizations struggle to define governance policies that both align to the business outcomes they are looking to accomplish and are tactical enough that they can be implemented and enforced by operational teams.
- **Data Landscape Visibility:** Finding everything that's important across multiple languages without high numbers of false positives and false negatives is hard, especially in unstructured and semi-structured data. Most organizations underestimate the amount of work this requires and don't appreciate how many types of sensitive data are missed by most commercial classification engines.

- **Regulatory Compliance Volatility:** Most organizations have data that's subject to an average of 3-5 different legislations. Adding to the complexity, new provincial, state, and federal legislations keep being added, and existing legislation is frequently updated.
- **Security Tool Efficacy:** Many security tools aren't data centric so validating the performance of the existing security infrastructure in terms of data protection may not align, which often leads to bias and a false sense of security.
- **AI/ML Enablement Risk:** Safely enabling artificial intelligence, machine learning and large language models (e.g., Copilot) requires the implementing organization to ensure all data used for processing is accurately classified and governed. Most organizations aren't doing this well.
- **Breach Mitigation and Resilience:** Developing robust Incident Response (IR) protocols to manage data breaches is a necessary part of a robust security strategy but isn't part of a traditional perimeter defense approach.

The Domestic Competitive Landscape

Within the Canadian market, several providers offer solutions critical to the data classification and governance journey. These players generally differentiate themselves through their core competency: Data Discovery, Security Tool Integration, or AI/Vertical Enablement. It's necessary for organizations to do their due diligence to identify the top solutions and evaluate each solution against business requirements and their ability to deliver a comprehensive, end-to-end solution. Some of the organizations that should be included in this evaluation are: Data & More, Cavelo, Varonis, BigID, Cyera, Concentric AI, OneTrust and Purview.

We will be exploring the following criteria:

1. **The foundation |** Searchers, crawlers, indexation and their consequences
2. **Data classification |** Key words, regular expressions, AI or Multi factor classification
3. **Data remediation |** Automation, workflows, data stewards, other considerations
4. **The opportunity for Canada**

1. The Foundational Imperative:

We teach children the timeless lesson of *The Three Little Pigs*, the necessity of building a strong, reliable foundation against future threats. For modern organizations, this lesson is more critical than ever.

A robust data foundation is essential, not just for defending against external threats (the "Big Bad Wolf" of compliance fines and breaches), but also for enabling productive initiatives like Artificial Intelligence. Without accurate data classification, any strategic endeavor built upon AI is inherently unstable. In addressing this fundamental need, the current market generally presents the following strategic options:

SEARCHERS / CRAWLERS

Legacy data discovery tools, such as Microsoft Purview and traditional crawlers, operate primarily on keyword-based scanning and Regular Expressions (RegEx). This approach inherently lacks the context required for reliable classification, leading to two major strategic failures:

1. **High Rate of False Positives:** Simple keyword matching fails to distinguish between data types. For example, the term "bonus" could be mistakenly flagged as financial, contractual, or project data. Similarly, a string matching a Canadian passport format might be a benign project ID. This results in analysis paralysis due to the sheer volume of irrelevant alerts.
2. **Resource-Draining Timelines:** Full repository scans often require weeks or months to complete. Furthermore, every subsequent search or compliance query initiates a new, manual process. The required manual sorting and validation after each scan results in unacceptable delays and significant operational expenditure, hindering immediate risk remediation.

Conclusion: Keyword-based searching is a time-consuming, context-blind methodology that undermines the accuracy and efficiency required for modern Data Loss Prevention (DLP) and compliance.

INDEXATION

The principle of fast retrieval, from indexing shared folders on a local file server to indexing enterprise unstructured data, is essential for efficiency. However, deploying a central data index for governance introduces new and significant security considerations that organizations must address:

- **Index Ownership and Control:** Where is the index physically located, who manages the underlying infrastructure, and what protocols are in place to protect the integrity of the indexed metadata?
- **Vendor Reliance and Data Exposure:** Is the vendor storing and controlling the indexed data? This necessitates a thorough vetting of their access controls and processing rights, particularly concerning data residency and sovereignty.
- **Data Processing and AI Use:** How does the vendor store and process the data? Are there auxiliary AI environments utilizing your indexed metadata for "learning" or product improvement purposes, introducing unintended data exposure?
- **Enforcement Mechanisms:** What explicit mechanisms are in place to ensure the index directly translates identification into immediate, automated data management and remediation?

While indexing reduces query times from months to mere seconds, it simultaneously introduces a new security surface. Relying on large vendors like Microsoft, Google, or Workday, all of whom have experienced breaches, increases the overall organizational risk. Every new dependency in the security ecosystem must be rigorously assessed for inherent risk.

2. Data Classification

Executive rhetoric demands data-driven decisions, yet leadership is consistently shocked by the true volume and location of sensitive data, including duplicated records, IP, PII, and security data—hidden across the enterprise. The fundamental strategic query remains: How can organizations discover and govern this crucial information before it creates liability via systems like Copilot?

REGULAR EXPRESSIONS

While a Regular Expression (RegEx) can define a basic search pattern, its limitation is the complete absence of context. A simple keyword query delivers an enormous volume of non-relevant matches (false positives) that must be manually triaged by the IT team across every document and message. This inefficiency is compounded by the fact that comprehensive security requires numerous parallel scans, a costly, incomplete and slow process that severely delays risk remediation.

Relying on Regular Expressions and proximity keywords for data classification is comparable to securing critical assets with a five-character password only, without also enabling Multi-Factor Authentication - it provides a basic level of security but that's not sufficient by today's security standards. This inherent lack of precision and contextual validation is the primary reason legacy classification technologies have developed a poor reputation and failed to deliver reliable security outcomes across the industry.

AI BASED CLASSIFICATION

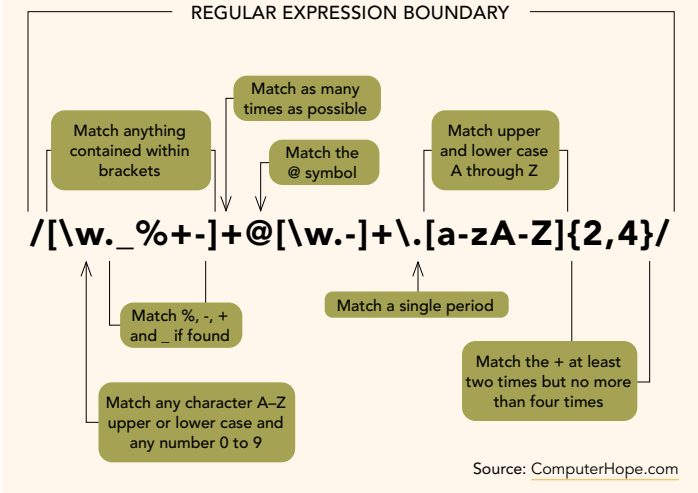
The transition to AI-based data classification introduces critical questions regarding data integrity and vendor transparency. The two major considerations are: the location and method of data processing, and the verified accuracy of the results.

A key operational challenge is the exorbitant cost of continuous AI processing. To remain competitive, some vendors resort to efficiency compromises, including data sampling, where only scanning a small subset of the total data and using the AI to apply generalized, unverified classifications across the remainder of the inventory is used. This introduces inherent data quality risk.

The other key concern with AI-based classification is consistency. Anyone that's used AI is familiar with 'hallucinations', where AI returns information that has nothing to do with the prompt it was provided. Every time this occurs equals a false positive, or even worse, a false negative in the classification.

This lack of trust and verified accuracy explains a strategic paradox: Many organizations utilizing AI for data classification deliberately shift their marketing focus toward the easier-to-sell security and enforcement features of their

Regular Expression E-mail Matching Example



platform, treating the underlying classification engine as an ancillary component.

MULTI FACTOR CLASSIFICATION (MFC)

MFC runs on Regexp+, but provides additional layers such as:

- **Context Mapping (RegEx+):** This feature applies advanced logic to keywords, requiring multiple criteria (e.g., start date, expiration date, facial image, and country-specific RegEx) before classifying sensitive data like PII. This approach guarantees significantly higher accuracy and reduces false positives by moving classification from "word matching" to "intent validation.
- **AI Augmentation:** (Not to be confused with AI-based classification). MFC uses AI to enrich preloaded classification dictionaries, tags, and definitions. This includes utilizing AI for multi-language translation, ensuring the meaning and value of data is consistently classified across diverse linguistic environments.
- **Human and Machine Validation:** MFC enables data stewards and custodians to review and validate search results and classification policies on the spot. This iterative, dual-feedback loop (human and machine teaching) ensures continuous refinement, elevating the quality and reliability of complex custom criteria (e.g., Intellectual Property or case data).

Quantification

The financial risk associated with data exposure can and must be quantified and visualized using established industry metrics, such as those published annually in the IBM Cost of a Data Breach Report 2025. Every piece of PII, PHI, and Intellectual Property (IP) existing within your environments represents a tangible risk (see table).

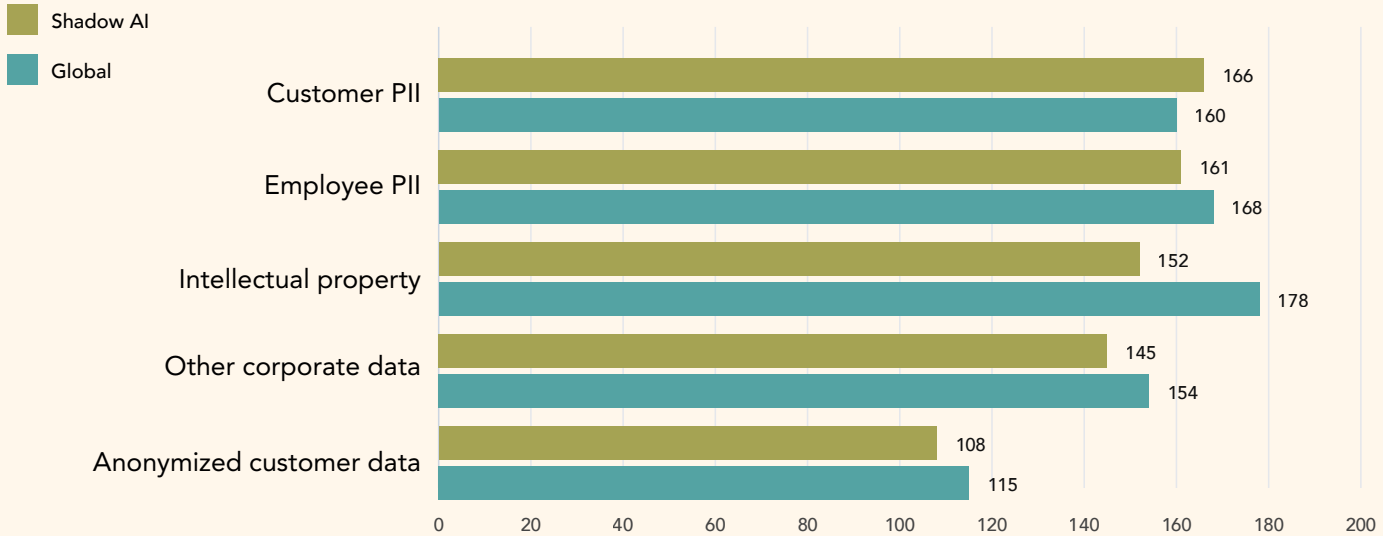
As breaches escalate in frequency, the strategy must pivot from solely securing the perimeter to applying granular security measures directly to the data itself.

This rigorous quantification of data risk provides the foundation for genuine data-driven decisions and the ability to accurately justify critical IT and security project budgets. Furthermore, it unlocks operational capabilities your organization has never accessed, such as:

- **Automated Data Subject Requests (DSRs):** Accurately locating all data related to an individual to meet tightening privacy laws.
- **AI Processing Compliance:** Precisely governing what data can and cannot be used for AI processing to comply with rapidly evolving AI regulations.

Financial Risk Associated with Data Exposure

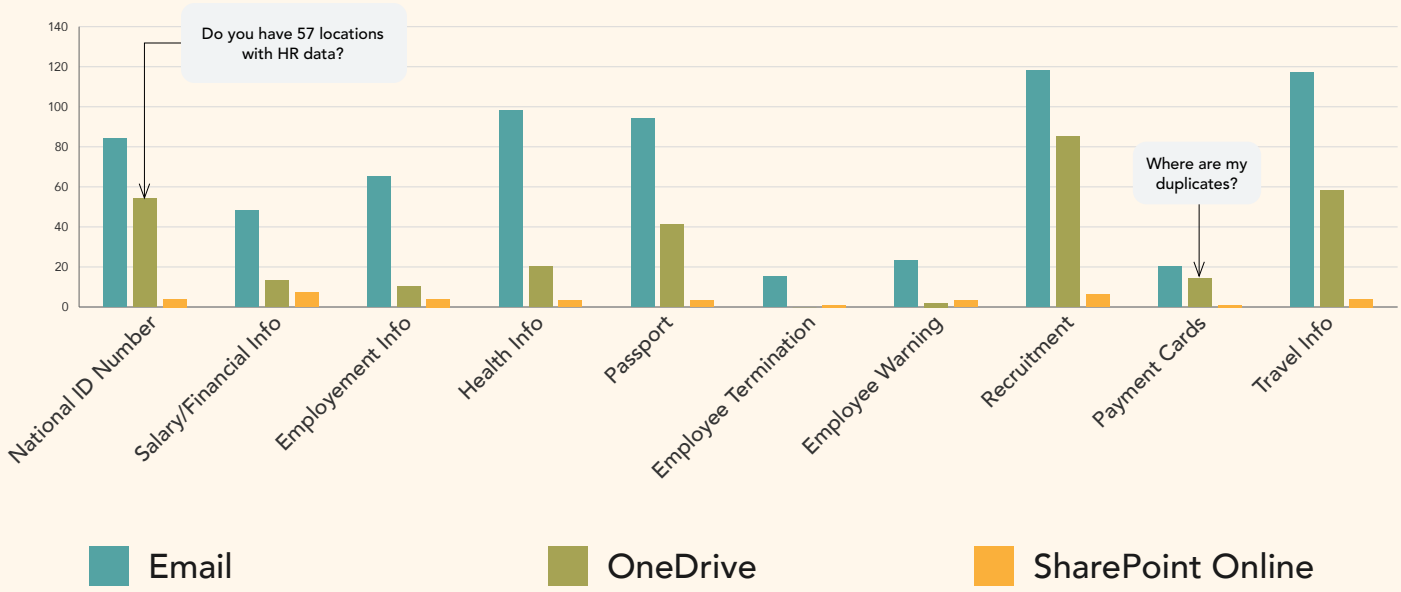
Measured in USD; more than one response permitted



Source: IBM Cost of a Data Breach Report 2025

The Sprawl Conflict: Not all organizational data is of equal value or importance. Once actionable discovery insights surface, conflicts immediately arise concerning retention, departmental ownership, and security protocols. Remediation is complex: One case study revealed recruitment data replicated across 83 locations (including email accounts), despite only one approved repository. This duplication and exposure demand nuanced governance, not simple deletion. See table for the data.

CASE STUDY: Where Sensitive HR-Related Data is Stored Across Different Systems



3. Data remediation

Accurate data classification is the fundamental intelligence layer of enterprise security, but it is incomplete without a rigorous, verifiable remediation framework. The challenge begins after sensitive data is identified. Unlike generic security actions, data remediation, the process of deleting, encrypting, or quarantining high-risk information, cannot be fully automated. This is due to the inherent complexity of data sprawl: high-risk PII or business data is often duplicated across unauthorized locations (e.g., file shares, email inboxes), yet some copies may be functionally legitimate. Simply pressing a delete button is an unacceptable governance liability.

This necessity for human-validated action elevates the role of the Data Custodian and Data Steward. The custodian, the individual accountable for a specific data set or repository, serves as the critical gatekeeper in the compliance workflow. A successful governance solution must move beyond simple alerting to define and engage these custodians at enterprise scale, providing them with a streamlined, context-rich workflow to:

1. **Review and Validate:** Verify that flagged data is, in fact, an unauthorized or expired copy.
2. **Approve Action:** Officially sign off on the deletion or migration of content.
3. **Ensure Accountability:** Record the action to maintain a legally sound audit trail for regulatory bodies.

By empowering custodians to own the last mile of data governance, organizations transform a state of "knowing their risk" into a state of continuous risk mitigation. This validated remediation is the only path to ensure that the enterprise data set is clean, compliant, and structurally sound for modern initiatives, including the safe and responsible adoption of Generative AI.

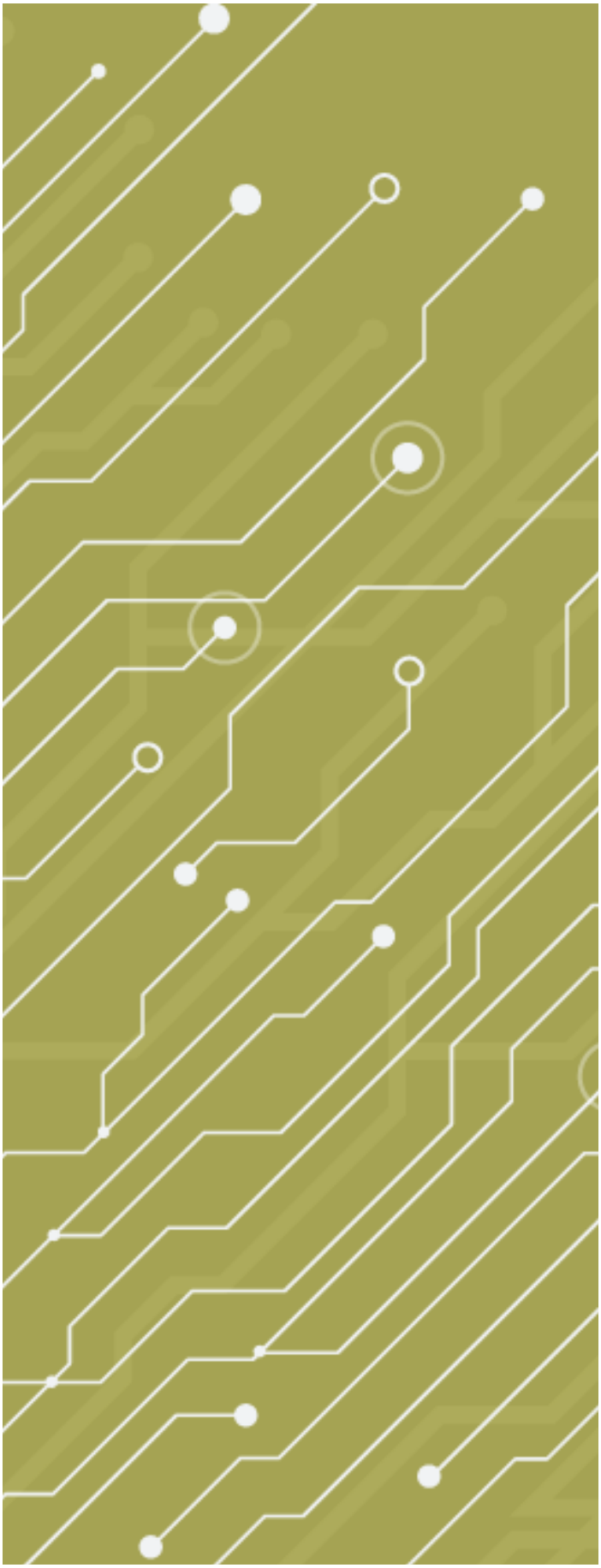
4. The opportunity for Canada

In periods of rapid technological change and uncertainty, it's difficult for IT leadership to maintain a clear vision and justify security spending to the business. When this happens, most organizations tend to stick with what's worked in the past. Unfortunately, security spending that focuses solely on securing the perimeter, is no longer sufficient. If they are willing to change, organizations can:

- Quantify their data and use the findings to justify the necessary changes in IT spending.
- Lay a solid foundation for AI agents to avoid joining the 95% of businesses with failed agentic AI projects.
- Take an approach that secures both the perimeter and their important data.
- Manage the complex, ever-changing compliance landscape.
- Be better positioned to address cybersecurity concerns, meet cyber insurance requirements, and effectively respond to data breaches and other data incidents.

Realizing these benefits starts with a change in mindset, with data at the core. Data classification and effective information management are the keys to success and will yield much greater returns than simply increasing the strength of perimeter security.

Jaap Mantel is a VP of Sales at Data & More ApS, overseeing the expansion into the North American market since December 2021. Previous experience includes roles as Director of Sales and Regional Manager Canada at LiveTiles, Head of North America at Wizdom, and Director of Partner Channel at Dynamic Owl Consulting, which was acquired by Skyvera.



Ten Insights into How AI Is Reshaping Cybersecurity in Canada

by David Masson, Presented by Darktrace

Cybersecurity is a field that's constantly on the move. The changing landscape keeps things interesting for practitioners, who are required to adapt constantly to new technologies and attacker methods. In recent years, however, the pace of change has accelerated sharply. Advances in AI are reshaping how cyber-attacks are developed, executed, and scaled, rewriting the terms of engagement between attackers and defenders. For today's security leaders, the challenge is in ensuring that their defences evolve as quickly as the threats they face.

Each year, Darktrace surveys over 1,500 security leaders worldwide to take the temperature of attitudes to AI in cybersecurity. We ask how AI is impacting the threats they face, how they are responding operationally, and where they believe AI is delivering the greatest value across prevention, detection, response, and recovery workflows. Over 100 of these cybersecurity professionals are based in Canada, spanning manufacturing, retail, financial services, technology, healthcare, and other critical sectors.

Now in its third year, the State of AI Cybersecurity survey reveals clear patterns and trends: While Canadian organizations increasingly see AI as essential to modern cybersecurity, many are still struggling with how to adopt it securely for maximum impact. In this article, we'll break down key findings from the Canadian data, including the top threats worrying CISOs, most popular uses of AI within the security stack, and the growing challenge of securing AI itself.

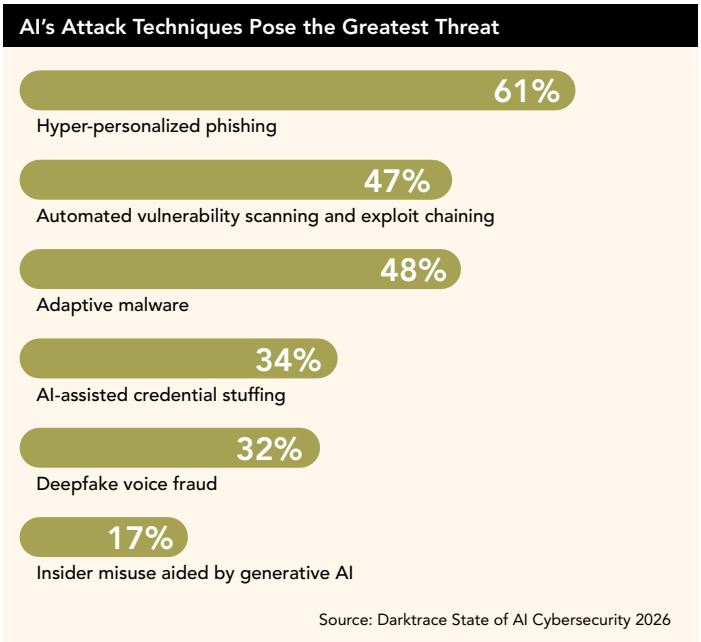
Key findings from the survey

1. AI IS SIGNIFICANTLY INCREASING THE SOPHISTICATION AND SUCCESS RATE OF SOCIAL ENGINEERING ATTACKS.

94% of respondents say that AI is making social engineering attacks, such as phishing, more effective. It follows then that 92% report that AI-powered cyber-threats are forcing security pros to significantly upgrade their tooling and processes. Following the widespread availability of ChatGPT, Darktrace observed a 135% increase in novel social engineering attacks, suggesting that generative AI was already providing an avenue for threat actors to craft sophisticated, targeted attacks at scale. As malicious activity increasingly blends in with legitimate user behaviour, organizations need security controls that can adapt in real time and distinguish subtle anomalies rather than rely solely on static rules or known indicators such as payloads.

2. AI IS ENABLING MORE TARGETED AND ADAPTIVE THREATS.

Respondents identified hyper-personalised phishing as the area where AI is having the greatest impact on threats (61%), followed by adaptive malware (48%), with automated vulnerability scanning and exploit chaining close behind (47%). It's no coincidence that all of these attack types are capable of evading traditional, signature-based defences, highlighting the importance of a defensive layer that can learn continuously and respond dynamically as threats evolve.



3. READINESS TO DEFEND AGAINST AI-POWERED THREATS REMAINS LOW.

Nearly half (45%) say they do not feel adequately prepared to defend against AI-driven cyber threats. While an optimistic 14% reporting being highly prepared, the outlook remains mixed. Respondents point to a lack of AI-specific knowledge, staffing constraints, and poor integration across security tools as key barriers, suggesting that improving readiness will require not just new technology, but simpler, more unified approaches that reduce complexity for already stretched teams.

4. AI'S GREATEST DEFENSIVE VALUE IS IN DETECTING THE UNKNOWN.

The majority of Canadian respondents (77%) believe novel threat detection and anomaly spotting is where defensive AI can have the greatest impact, followed by threat intelligence enrichment (52%) and automated response and containment (46%). However, only 22% recognize AI's potential to significantly enhance analyst productivity, pointing to an awareness gap that may be limiting how effectively organizations use AI to reduce decision fatigue and enhance analyst productivity.

5. GENERATIVE AI IS WIDESPREAD, BUT DEEPER AI TECHNIQUES REMAIN UNDERUSED.

Generative AI and large language models are now used in 89% of Canadian security stacks, reflecting rapid adoption for tasks such as summarization, investigation support, and reporting. By contrast, only 21% say they are leveraging unsupervised machine learning. Unsupervised approaches typically underpin behavioural analysis, enabling the detection of more subtle, targeted, or payload-less threats that abuse trust and normal business processes, such as vendor compromise or insider-driven activity.

6. MANAGED SECURITY SERVICES ARE BECOMING THE PREFERRED OPERATING MODEL.

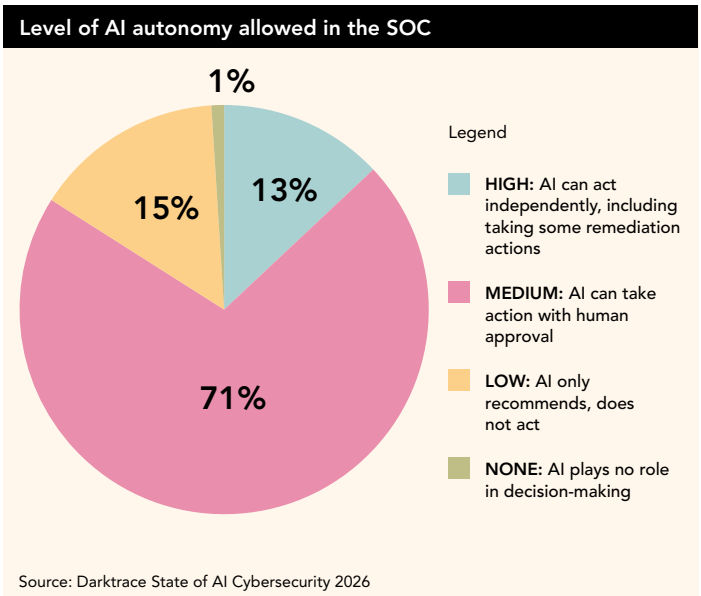
There is a notable shift towards outsourcing security operations, with 88% of Canadian respondents preferring to acquire new SOC capabilities through a managed service rather than deploying and managing tools in-house. This reflects ongoing skills shortages and operational strain, as well as the appeal of 24/7 coverage, faster time to value, and access to specialized expertise, allowing internal teams to focus on higher-value strategic and investigative work instead of day-to-day alert management.

7. DATA PRIVACY REMAINS A DECISIVE FACTOR IN DEFENSIVE AI ADOPTION.

The majority of Canadian security professionals (86%) say they prefer defensive AI solutions that do not require their organization's data to be shared externally. This reflects ongoing concerns around data sovereignty, regulatory compliance, and exposure of sensitive information, and reinforces the importance of AI approaches that can learn and operate within an organization's own environment without relying on centralized data pooling.

8. CAUTION REMAINS AROUND FULLY AUTONOMOUS AI IN THE SOC (SECURITY OPERATIONS CENTER).

Most Canadian respondents (71%) say they are limiting the autonomy of AI-driven actions in the SOC until explainability improves, while only 13% are comfortable allowing AI to act independently without a human in the loop. This hesitation highlights a trade-off: If security leaders are confident that actions are transparent, proportionate, and align with business risk, autonomous remediation can significantly reduce response times, contain threats before they escalate, and relieve pressure on analysts during high-volume incidents.



9. CONCERN IS GROWING AROUND THE SECURITY OF ENTERPRISE AI USE.

One third of Canadian security professionals say they are extremely or very concerned about the security implications of employees using in-house LLMs or custom models. That concern rises to 49% for third-party tools such as ChatGPT and Copilot, and 46% for AI agents. Sensitive data exposure is the top worry, followed by potential violations of security and privacy regulations. This focus is well founded: 53% of breach incidents involve Personally Identifiable Information (PII) (IBM Cost of a Data Breach Report 2025). These breaches remain among the most common and costly, and can trigger regulatory fines alongside lasting reputational damage.

10. FORMAL GOVERNANCE FOR AI USE REMAINS THE EXCEPTION RATHER THAN THE NORM.

Only 35% of Canadian organizations report having a formal policy governing the safe and secure use of AI, while 10% say they have no plans to put such structures in place. As AI becomes embedded across business and security functions, the absence of clear governance increases the risk of data misuse, compliance failures, and inconsistent decision-making. Establishing guardrails around how AI is adopted, monitored, and controlled is increasingly essential to ensure innovation does not come at the expense of security or trust.

The survey findings make one thing clear: AI has become a defining force in cybersecurity, shaping both the threats organizations face and the defences they must build. While Canadian security leaders recognize AI's potential to improve detection, response, and resilience, many remain underprepared, constrained by skills gaps, tool sprawl, and limited governance. Caution around autonomy and data sharing is prudent, but inaction carries its own risk as attackers seek to blend more seamlessly into normal business activity. The organizations best positioned to succeed will be those that adopt AI systematically – pairing adaptive, behaviour-based defences with clear policies and oversight – to keep pace with the new era of AI-driven threats.

Interested in the global picture? Look out for the State of AI Cybersecurity 2026, coming soon from Darktrace.

David Masson is a VP, Field CISO at Darktrace, and has decades of experience working in fast moving security and intelligence environments in the UK, Canada and worldwide. With skills developed in the civilian, military and diplomatic worlds, he has been influential in the efficient and effective resolution of various unique national security issues. At Darktrace, David advises strategic customers across North America and is also a regular contributor to major international and national media outlets in Canada where he is based.

How Leadership Decisions Make Cyber Breaches More Expensive

by Mary Carmichael

Breach costs are leadership outcomes

Most cyber breaches do not begin as crises. They begin with routine business decisions, a configuration change approved quickly, a trusted vendor operating with limited oversight, or a software update deployed faster than governance allows. Whether these moments remain contained or escalate into multi-million dollar losses is determined long before the incident, by leadership choices around risk ownership, vendor concentration, insurance structure, and accountability.

IBM's Cost of a Data Breach 2025 report estimates the average global breach at about $4.44 million, with costs driven more by business disruption, prolonged recovery, and post-incident remediation.

The data explains why: 86% of organizations experience disruption, 65% do not fully recover, and nearly a quarter take more than four months to resume normal operations. These outcomes show that breach costs depend less on how an incident occurs and more on how prepared an organization is to respond and recover.

Breaking it Down

65%	of organizations have not fully recovered.
86%	of businesses experienced disruption.
$5.52m	average cost of a data breach for organizations that didn't use security AI and automation.
24%	of organizations took 126–150 days to recover.

Source: IBM Cost of a Data Breach Report 2025

That is why cyber risk is not simply an IT expense, but a balance-sheet liability, influenced by earlier decisions around insurance coverage, third-party reliance, governance, and accountability. Breaches may be inevitable; financial disasters are not.

Cyber risk is an enterprise issue

Cyber incidents are no longer just IT issues; they directly impact operations, capital allocation, customer experience, and leadership accountability.

- **For CFOs, breaches are capital events.** Insurance premiums, uninsured losses, business interruption, and regulatory remediation compete for limited resources, immediately affecting cash flow, reserves, and forecasts.
- **For boards, cyber risk is a governance issue.** Regulators and shareholders evaluate vendor reliance, insurance terms, and oversight frameworks as fiduciary decisions—not technical details.
- **For CIOs and technology leaders,** the role is translating technology choices into business exposure, as digital platforms are now embedded in revenue and core operations.
- **For business leaders outside IT,** cyber risk becomes real when operations stop, when payments are delayed, customers must be notified, or work halts due to platform failure.

What unites these perspectives is this reality: breach costs don't stay where the failure occurred; they spread across the business, exposing decisions made for speed, efficiency, or cost savings without accounting for risk.

What do breaches really cost?

When executives assess the cost of a cyber breach, they typically focus on immediate expenses such as incident response teams, forensic investigations, legal counsel, system restoration, and crisis communications. However, these costs are only a fraction of the total financial impact.

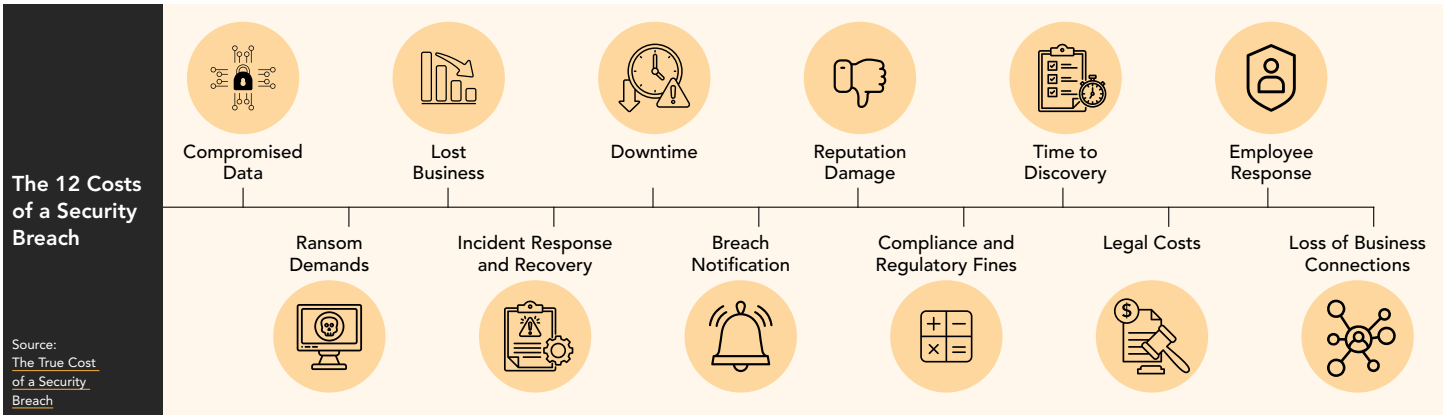
In the months following an incident, costs frequently increase rather than decline. Insurance recoveries are often reduced by exclusions, limits, and documentation requirements. Vendor liability is constrained by contract terms. Regulatory scrutiny shifts from technical root causes to governance, oversight, and accountability. Recovery timelines extend as third parties influence remediation schedules, while executive time is increasingly consumed by investigations, disclosures, remediation planning, and ongoing stakeholder engagement.

Six to twelve months later, organizations often realize the breach has permanently changed how they operate. Short-term response expenses turn into ongoing costs for compliance, legal support, monitoring, and controls. Growth initiatives slow as capital and leadership attention shift to risk management. As the image shows, the true cost of a breach extends well beyond system recovery to include lost business, reputation damage, and sustained strain on employees, making the incident a lasting business issue, not a one-time event.

A Case Study: Change Healthcare

The 2023 ransomware attack on Change Healthcare, a critical payments and claims-processing provider used by hospitals, pharmacies, and insurers across the United States, shows how quickly costs can compound. In the immediate aftermath, attention focused on restoring systems and supporting customers as prescription processing stalled and healthcare providers faced delays in reimbursement.

As time passed, the financial impact expanded significantly. UnitedHealth Group, Change Healthcare's parent company, has reported more than US$2 billion in related costs across subsequent quarters, driven by business interruption, customer support, system rebuilds, remediation programs, and longer-term operational changes. The final bill reflects months of disruption across a tightly interconnected ecosystem, where cash flow constraints, delayed transactions, and erosion of operational trust proved far more expensive than the initial incident response. The breach revealed how deeply business continuity now depends on shared digital systems and partners.



Does cyber insurance cover most breach costs?

TELUS's Canadian Ransomware Study and Canadian Cyber Insurance Study indicate that, on average, cyber insurance claims cover 60% of an incident's direct response and recovery costs. Most of the longer-term expenses such as system modernization, expanded security programs, regulatory remediation, and business impacts such as delayed transactions or lost revenue are absorbed directly by the organization. Cyber insurance can cushion the initial shock of an incident, however, it does not fund months of disruption or years of remediation.

The leadership assumptions that quietly inflate breach costs

What turns an incident into a major loss is rarely the specific control that failed. It is the business decisions made upstream such as concentrating critical functions with a single vendor, automating processes without fallback options, or underinvesting in recovery planning that leave the organization with little ability to absorb disruption when something goes wrong.

ASSUMPTION 1: "CYBER INSURANCE WILL COVER THE LOSS"

Cyber insurance is often treated as risk transfer. In practice, coverage is conditional, limited, and frequently narrowed when incidents involve third parties or systemic disruption. Policies require specific controls to be implemented and consistently operated and coverage typically narrows when incidents involve third parties, shared platforms, or widespread disruption.

The City of Hamilton's 2024–2025 cyber incident illustrates this clearly. By mid-2025, the city reported recovery costs of about $18.3 million, while $5 million in cyber insurance claims were denied after the insurer determined that multi-factor authentication, required under the policy, had not been fully implemented. The financial exposure did not disappear; it shifted back to the municipality and its taxpayers.

KEY TAKEAWAY:
Cyber insurance softens the impact; it does not eliminate the risk.

Leaders should ask how their cyber policy would perform in a real breach. Then, they should then test that assumption by walking through realistic scenarios with their broker, confirming that required controls are operating in practice, and understanding how coverage shifts when third parties or shared platforms are involved. Any gap between policy expectations and operational reality should be viewed as financial exposure, not technical debt.

ASSUMPTION 2: "WE'LL HAVE TIME TO DECIDE DURING THE INCIDENT"

Many assume that critical decisions can be made once an incident is underway. The expectation is that leadership will have time to gather facts, evaluate options, and determine the right course of action as events unfold.

The Equifax breach illustrates the cost of this assumption. Post-incident investigations found that while technical issues triggered the breach, some of the most damaging impacts emerged from how the incident was escalated, communicated, and governed. Decisions around internal notification, public disclosure, and regulatory engagement were slow and inconsistent, reflecting the absence of a rehearsed decision framework at the leadership level. The result was prolonged uncertainty, intensified regulatory scrutiny, and significant reputational and financial damage on top of the initial technical failure.

KEY TAKEAWAY:
Decisions made in advance determine outcomes under pressure.

Do the hard work before an incident occurs. Assign who can shut systems down, who engages insurers and regulators, who approves public disclosure, and what triggers each decision. Document these choices, test them in realistic scenarios, and update them as the business changes.

ASSUMPTION 3: "VENDOR RISK ENDS AT THE CONTRACT"

Vendor risk is often treated as a one-time procurement decision. Well-known brands and signed contracts create confidence that risk has been transferred. It has not. Organizations remain accountable for how third-party platforms are configured, integrated, and used, particularly where data, regulation, revenue, or operations are involved.

Risk continues to evolve after contracts are signed as defaults persist, features expand, and data flows change. Early use of Zoom exposed how convenience-driven default settings led to unintended data exposure, with consequences borne by customers rather than the vendor. AI platforms follow the same pattern at greater scale. Many organizations adopt them without fully understanding where data is stored, how prompts and outputs are retained, or whether information is used for model training.

KEY TAKEAWAY:
Treat vendor reliance as an ongoing business risk

Vendor risk is never outsourced. Brand reputation, certifications, and contracts may reduce uncertainty, but accountability always remains with the business. Leaders should treat critical vendors

and AI tools as ongoing operational dependencies, not one-time purchases, with clear ownership for configuration and data use, regular reviews of changes and defaults, and explicit authority to approve or block material risk changes.

ASSUMPTION 4: "SYSTEMIC CLOUD FAILURE IS TOO REMOTE TO PLAN FOR"

Systemic technology failure was once considered theoretical. Today, it is an operational reality. As organizations concentrate critical functions on a small number of cloud, SaaS, and AI providers, disruption no longer requires a cyberattack.

Recent incidents make this clear. Outages at major cloud providers have disrupted airlines, retailers, banks, and hospitals without any malicious activity. The 2024 CrowdStrike update incident made this tangible. A faulty content update in a widely used endpoint security product caused mass outages across airlines, banks, hospitals, and governments.

This is concentration risk. When large numbers of organizations rely on the same platforms for identity, infrastructure, analytics, or security, isolated failures quickly become systemic events. As businesses further integrate shared vendors, data pipelines, and AI-driven systems, failures become harder to isolate, slower to fix, and significantly more expensive to recover from.

KEY TAKEAWAY:
Plan for concentration risk, not just breaches

Leaders should assume that shared cloud and AI providers will fail and that recovery will be slower and more complex than in isolated incidents. This starts with identifying which providers the business cannot afford to lose, understanding what would stop operating, and developing practical playbooks, including manual workarounds and communication plans. Systemic technology risk is no longer hypothetical; it is a feature of modern digital business.

ASSUMPTION 5: "CYBER IS A TECHNICAL ISSUE, NOT A BUSINESS ONE"

This is often the most expensive assumption of all.

When cyber risk is framed as technical, accountability drifts away from the business. Board discussions focus on controls, while harder questions about vendor dependency, insurance exposure, contractual liability, and decision rights receive less attention.

The 2023 MGM Resorts cyber incident illustrates this dynamic. A social-engineering attack disrupted casino and hotel operations across multiple properties, leading to extended system shutdowns and manual workarounds. Reported losses exceeded US$100 million, driven by lost revenue and operational disruption rather than the cost of technical recovery. Public and investor attention focused not on how the attack worked, but on leadership preparedness, governance, and decision-making.

Incidents like this reflect a broader shift. Markets and regulators no longer view cyber events as IT failures; they assess them as management failures. The questions being asked are about judgment: what risks were accepted, where dependencies were allowed to concentrate, and which leadership decisions amplified the impact.

KEY TAKEAWAY:
Cyber risk is an enterprise risk

Manage cyber risk like any other enterprise risk that affects revenue, cash flow, and valuation. Assign a single executive owner accountable for outcomes, integrate cyber exposure into enterprise risk and capital planning, and review decision-making, dependencies, and recovery performance after incidents, not just technical failures.

A Leadership Playbook for Reducing Breach Costs

Reducing the cost of cyber incidents is not a technology challenge; it's a leadership one. Organizations that limit financial damage are those that make clear decisions about risk before an incident occurs.

- **Stress-test cyber insurance against real scenarios.** Evaluate coverage under realistic events such as vendor failures and widespread outages, not just at renewal. Treat uncovered scenarios as retained financial risk.
- **Map critical vendors as operational dependencies.** Identify which cloud, SaaS, and AI providers the business cannot operate without, understand the financial impact of their failure, and make that concentration visible to the board.
- **Watch for risk drift, not just compliance.** Move beyond periodic audits and require visibility into how configurations, data use, and platform features change over time.
- **Plan for systemic failure, not isolated breaches.** Assume shared providers will fail and recovery will be constrained. Define how the business will operate, communicate, and prioritize during prolonged disruption.
- **Use incidents as governance signals.** After every incident or near miss, change at least one decision, contract, or oversight practice. If nothing changes, risk remains.

Conclusion: Cyber incidents are inevitable. How costly they become is not.

The difference between a brief disruption and a value-destroying crisis is rarely attacker sophistication. It is leadership decisions made in advance, about insurance, vendor concentration, operating dependencies, escalation authority, and accountability. When those choices are vague or overly optimistic, costs compound quickly and control disappears.

Markets, regulators, and customers now treat cyber incidents as tests of management judgment, not technical failure. The path forward is deliberate decision-making: bringing cyber risk into capital allocation, vendor strategy, and enterprise risk discussions, and defining in advance who decides what when trade-offs collide. Organizations that do this retain control under pressure; those that do not are rarely surprised by the breach, only by how little control they have over the cost.

Mary Carmichael is the Managing Director of Risk Advisory at Momentum Technology, with over 15 years of experience helping organizations turn digital risk into strategic advantage. She has advised leaders across higher education utilities government and energy on cybersecurity maturity emerging technology risk IT governance and cloud transformation.

Facilitating Cyber Crisis Tabletop Exercises: Insights from the Front Line of Simulation Leadership

by Simon Hodgkinson, Presented by Semperis

Across private industry and the public sector, organisations are confronting an unprecedented level of operational risk originating from sources outside their control.

In the cyber space, threats rapidly evolve in scale, sophistication, and impact. Advanced by AI-powered tools and increasingly aggressive criminal groups (e.g., ShinyHunters, Scattered Spider), ransomware, supply chain compromise, identity-based attacks, and data breaches now routinely disrupt operations, reputations, and regulatory standing.

Simultaneously, organisations face increasingly complex and unpredictable threats from geopolitical instability, economic fragmentation, and environmental disasters caused by climate change.

The convergence of these forces has elevated cyber risk to a board-level concern. Organisations are keenly aware that their responsibility is not just to defend against these threats, but to ensure that when a cyber crisis occurs, they are prepared to respond, recover, and resume business operations as quickly as possible.

Decisions made in the first hours of a crisis can shape shareholder confidence, customer trust, brand reputation, and long-term resilience. Even more important are decisions made before a crisis. Planning and preparation are essential for a swift response and speedy recovery.

However, without regular practice, even the best-prepared teams can falter under the pressure of a real-world cyber

incident. A 2025 Semperis study, *The State of Enterprise Cyber Crisis Readiness*, revealed that although 96% of global organizations say they have a cyber response plan, 71% still experienced at least one incident that stopped critical business functions.

96%

of global organizations say they have a cyber response plan,

71%

still experienced at least one incident that stopped critical business functions.

As a facilitator of cyber crisis tabletop exercises, I've stood at the intersection of strategy, psychology, and operational readiness. These simulations are more than technical rehearsals. They are designed to challenge leadership thinking and bridge the gap between the cyber security team, operational leaders, and stakeholders.

This brief provides a firsthand perspective on facilitating tabletop exercises, drawing on real-world experience across sectors. It outlines strategic outcomes, facilitation techniques, and common challenges with the aim of helping executive teams understand the value of simulation-based preparedness and the role of the facilitator in driving meaningful impact.

Although the focus here is on cyber incident response, the insights and learnings are applicable across any crisis. After all, a cyber crisis is just a trigger for a bigger business crisis.

The Facilitator's Perspective

The role of a cyber tabletop facilitator is to guide diverse stakeholders through complex, high-stakes scenarios that test not just systems, but culture, communication, process, and decision making under pressure.

Over the years, I've facilitated exercises across sectors. Each session brings its own dynamics, but the core objectives remain consistent:

- Aligning cross-functional teams
- Maintaining realism
- Ensuring restoration of minimum viable business operations—as soon as possible

To drive these and other meaningful outcomes, the facilitator must ensure all stakeholders, responders, and involved participants emerge from the exercise with:

- A clear understanding of gaps in the response plan
- Steps for continuing to enhance their response processes
- Goals for educating their people
- Trust in their technology decisions

Facilitator Techniques: Setup and Common Challenges

My primary focus during the tabletop exercise is business resilience—not technology.

Businesses constantly change, and the technology platforms, applications, and systems that are in place during this quarter's tabletop or simulation will also change, evolve, or be removed by next quarter. Whether I'm running the simulation for executive or technology teams, I always challenge them to focus on the business outcome: How will we continue to operate during and after this crisis? How will we continue to sell groceries, deliver patient care, drill, or fly planes?

During the exercise, I continually observe, then inject questions to prompt discussion about how actions taken during a crisis will affect the outcome. For instance, how will a particular decision impact our revenue, employees, or brand?

While I go into the exercise with a clear agenda on inject pacing, I also allow flexibility for productive conversation to close "rabbit holes." In those conversations, participants discover critical details and gaps that they aren't aware of,

and working through the questions can clarify the impact of decisions.

The most important piece of advice I would offer is to consider diverse perspectives. I try to draw in the opinions of everyone in the crisis team. Teams must operate in command and control; however, that does not preclude listening to the "quietest voice in the room."

With the objective of business resilience firmly in mind, I move on with the crisis tabletop exercise. Here are four critical challenges that teams typically encounter.

1. VARYING LEVELS OF PREPAREDNESS

I typically start the tabletop with the executive team—and deliberately do not invite technical teams initially.

Executives often arrive with differing assumptions about their role in a cyber crisis. Some expect to delegate; others overstep. This misalignment can stall decision making. During a crisis simulation, a technical team representative provides situation reports and asks for prioritisation while the executive manages the business impact.

In a real crisis, it becomes clear why the separation of the executive team (who are managing the business) and the technical team (who are managing incident response) is critical. It's essential to allow space for the technical team to focus on containment and recovery. Communication and collaboration at the *right time* in the *right context* is key to success.

In a recent tabletop exercise with a multi-billion-dollar company, we spent significant time at the outset outlining roles, expectations, and escalation paths. While this could have been achieved through a pre-brief, walking through the process helped everyone understand why it's important to establish clear roles, responsibilities, and delegation *before* a crisis happens. In this case, the CEO stepped in and appointed one of the team as Crisis Director; through the exercise we were able to remind the CEO that his input was valuable but that he was not the decision maker.

Throughout the exercise, the injections progressively escalate to provoke robust discussion—and here we see the true depth of preparation to make on-the-spot decisions that directly affect not only the crisis outcome but also business resilience and continuity.

For example, the classic question to inject, from a cyber perspective, is, "Who decides if we pay a ransom, and on what basis do we make that decision?"

In a tabletop exercise, it is easy to take the moral and ethical position that the company will never pay ransom. At this point, I turn up the pressure to challenge that assumed response with real-world examples of companies that have lost their digital platform for weeks. I ask, "Would this business be able to survive?"

The answers are not always clear cut, and the reasoning behind decisions is affected by multiple variables. The 2025 Ransomware Risk Report from Semperis reveals that bad actors are constantly finding new ways to force ransom payments.

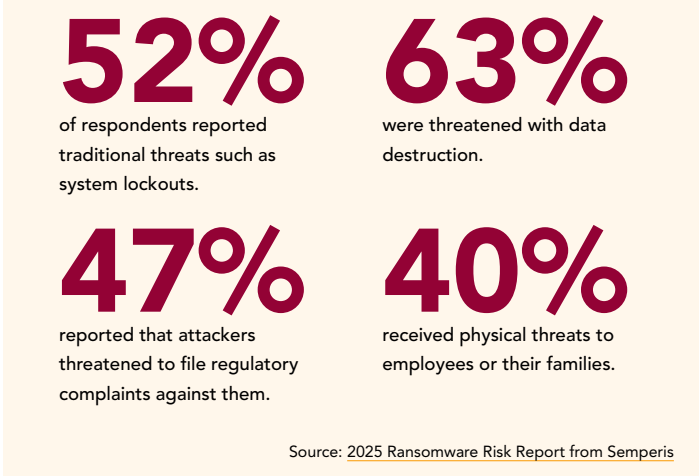
- 52% of respondents reported traditional threats such as system lockouts.
- 63% were threatened with data destruction.
- 47% reported that attackers threatened to file regulatory complaints against them.
- 40% received physical threats to employees or their families.

Cyber crisis preparation must include understanding of both the business impact and the human impact. That leads us to the second common challenge.

2. OVEREMPHASIS ON TECHNOLOGY

In both executive and technical cyber crisis tabletop exercises, there's a tendency to default to discussing technology while neglecting reputational, legal, and human dimensions. The technology is only as good as the process and the people managing and using it.

Methods of Bad Actors in Finding Ways to Force Ransom Payments



Source: 2025 Ransomware Risk Report from Semperis

The best tabletop scenarios focus on non-technical stresses on decision making, such as:

- Media leaks
- Shareholder pressure
- Environmental disasters
- Safety

I ensure legal, communications, HR, and business leaders are active participants, not observers. We must remember the cybersecurity team is generally doing incident response on a daily, weekly, and monthly basis. They know what to do. Where they need the most help is in focusing on operational priorities—and ensuring they have the support of the leadership team and stakeholders.

For example, in a tabletop exercise I conducted for a major UK firm, a simulated ransomware attack prompted heated debate—not about recovery, but about whether to inform the regulator and suppliers. The participants critically ignored the employees despite the HR Director's protestations. The takeaway for them was that it is critical for the incident commander to make sure all voices are heard.

It is also critical to make sure all voices know their roles before, during, and after a cyber incident. Lessons learned come from all participants, not just the cybersecurity team. Keep in mind, while cyber teams are responding and managing the technical aspect of the incident, forensics, logging, and so on, business stakeholders are focusing on trying to keep the business running as technology is restored.

3. DECISION PARALYSIS UNDER PRESSURE

As the tabletop exercise progresses and the injections escalate, the time window reduces, increasing the pressure on decision makers. This can lead to paralysis.

For example, a bad actor may escalate pressure by increasing the ransom demand, informing the regulator, informing your clients, or shortening the deadline for detonation of the malicious payload.

In a simulation, this drives deeper thinking across non-technical teams.

- Communications teams must prepare external and internal communication.
- Legal teams must ensure the right people have been informed in appropriate jurisdictions.
- Business leaders must know how to sustain business operations.

Each response team needs to listen and understand the perspective of the others. How does one reaction or decision impact other teams, services, business lines, and participants?

Often the immediate reaction on the technical side is to shut down external access to the digital ecosystem. However, in today' s world that means the business stops operating. Many high-profile, non-targeted attacks such as NotPetya and WannaCry spread in as little as 20 minutes. The phenomenal pressure that such a timeframe creates makes it clear why designating authority to mitigate cyber risk *in advance* is essential.

For many organisations, that realisation occurs during tabletop scenarios. Empowering the CIO or CISO to respond and contain or mitigate an attack may ultimately save many days—or even weeks—of downtime. However, the reverse should be considered. If they over-respond and impact business operations, it is critical that the reasoning behind the decision is understood so that they are supported and not vilified.

4. ASSUMPTION THAT EXISTING TECHNOLOGY IS AVAILABLE

During most tabletop exercises, the assumption is that standard communication systems will continue to work.

Organisations instinctively reach for familiar tools, only to realise they haven't rehearsed alternatives. Every day, they use email, collaboration apps such as Microsoft Teams, mobile messaging apps, and file sharing platforms such as SharePoint and Dropbox. And they expect those will always be available.

It's likely everyday systems *won't* be available in a crisis. And we must assume that even if these platforms are available, they are compromised—and therefore any communication is freely available to the threat actor.

In a simulation, we quickly establish the need for a totally isolated communications platform. The default tends to be WhatsApp. However, while WhatsApp might serve us well personally, it lacks corporate governance controls, which significantly impacts the forensic investigation and legal discovery process. Likewise, it does not have corporate access and authentication controls, potentially leading to inappropriate access.

Organisations also assume their incident response playbooks will be available; however, they are often on corporate systems that are either shut down or inaccessible when the incident response team isolates the corporate platforms from the internet.

Large, complex organisations also use a variety of tools and systems to communicate with staff and suppliers, and those also may no longer be available—or may create a disjointed response effort.

While none of these system breakdowns would be an issue for a non-cyber crisis, they are a huge issue during a cyber crisis, highlighting the need to prepare a totally isolated crisis management platform. The crisis response platform should be used for cyber and non-cyber incidents so that all teams across the organisation build familiarity.

As a facilitator, my role is to surface these blind spots early, prompting teams to codify contingency channels and ensure that crisis communications can continue even when primary systems are unavailable.

Post-Exercise Debrief

The debrief is a critical part of the tabletop exercise process. I conclude the exercise, take a break for 30 minutes, and ask people to reflect.

While every exercise results in different findings, a few common revelations invariably appear. Organisations discover they must immediately:

- Establish pre-approved communications templates
- Define delegations of authority
- Eliminate over-reliance on individual expertise versus team protocols
- Select and implement an isolated crisis management platform
- Create processes for documenting, logging, and justifying decisions
- Overcome reliance on technology working as it should

Now Is the Time to Transform Crisis Management

A successful cyber crisis tabletop exercise should be challenging and identify gaps in people, processes, and technology. The environment should feel pressurised and uncomfortable for those taking part—because that is the reality of crisis management.

Facilitating cyber tabletop exercises is part art, part architecture. It requires empathy, strategic foresight, and the ability to provoke without destabilising. My goal is always the same: to help leaders rehearse the unthinkable so they can respond with clarity when it counts.

These exercises don't just test systems—they reveal character, culture, and capability. And when done right, *they transform organisations from reactive to resilient*. A reasonable targeted approach is a great starting point. Be focused, be open, and record the critical findings.

Simon Hodgkinson is the former Chief Information Security Officer (CISO) at BP (formerly British Petroleum). He was responsible for cybersecurity including strategy, governance, architecture, education, counter-threat operations, and incident response. Simon currently combines advisory and executive roles for several organisations, including Semperis, Onyxia, Cyera, and ISTARI.

semperis

Run your next tabletop with Ready1

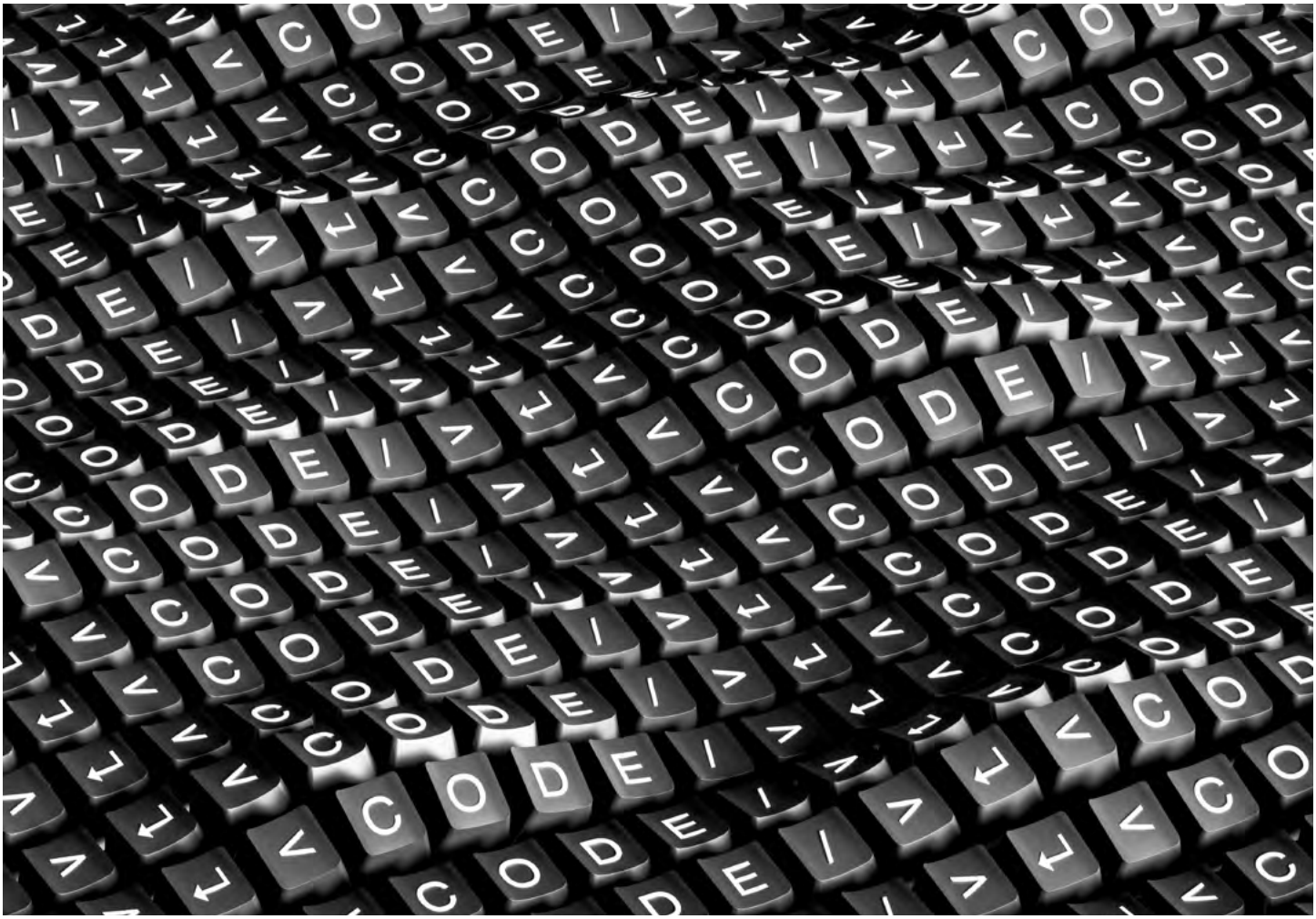
Don't assume your plan will work. Prove it.

- Make **tabletop exercises realistic**—include business leaders.
- Shift focus from more hires to **better coordination**.
- Store and share response plans **in out-of-band systems**.
- **Kill the complexity**: Too many tools = chaos.
- Treat **cyber threats** like any other **enterprise crisis**—because they are.

REQUEST ACCESS TO READY1 TODAY

r1

semperis.com/ready1



Post-Quantum Cryptography (PQC): The Looming Cryptographic Shift

by Munis Badar

Introduction: The Quantum Countdown Has Begun

The entire digital certificate (PKI) ecosystem, built on the foundations of RSA and ECC, is now on a countdown clock. With quantum computing advancing, Shor's algorithm will eventually break the cryptographic core of today's PKI. This urgency is driven by the "harvest now, decrypt later" threat, where adversaries can steal and store encrypted data including to decrypt once a quantum computer is available.

To address this, the cryptographic community has undertaken the largest transition in history: Post-Quantum Cryptography (PQC). PQC algorithms are designed to resist both classical and quantum attacks, relying on hard problems such as lattices and hash-based constructions.

The NIST PQC standardization process, launched in 2016, has now reached critical milestones with NIST finalizing on the selection of three ciphers:

- FIPS 203 (CRYSTALS-Dilithium) for digital signatures, FIPS 204 (CRYSTALS-Kyber) for key encapsulation, and FIPS 205 (SPHINCS+) for hash-based signatures.
- FALCON, another lattice-based signature scheme, was selected and will be published as FIPS 206
- HQC (Hamming Quasi-Cyclic) as documented in NIST IR 8545.

Enterprises, governments, and vendors must now plan for a decades-long transition: inventory cryptographic assets,

adopt hybrid certificates that combine classical and PQC primitives, and coordinate with ecosystem partners to ensure interoperability.

History shows that new cryptography often reveals hidden vulnerabilities years later, meaning flaws remain a real risk.

The risks of PQC adoption: algorithm maturity, performance overhead, interoperability gaps, and compliance uncertainty; must be mapped across the PKI lifecycle (issuance, renewal, rotation, revocation, archival). Strategic approaches such as crypto-agility, automation of certificate management, and staged rollouts are essential to navigate this transformation safely.

PART 1 | The Inherent Risks of PQC: Why This Transition is Fundamentally Different

THE UNPRECEDENTED SCALE OF CRYPTOGRAPHIC MIGRATION

Previous cryptographic transitions, such as the move from DES to AES or from SHA-1 to SHA-2 affected specific algorithms within established cryptographic paradigms. The PQC transition is fundamentally different in both scale and nature:

- **Paradigm Shift, Not Incremental Improvement:** We are not merely replacing one symmetric cipher with another faster or more secure one. We are replacing the entire asymmetric cryptographic foundation upon which digital trust is built. This affects every layer of the protocol stack, from hardware security modules and operating system libraries to application code and network protocols.
- **Global Simultaneous Transition:** Unlike previous transitions that could be managed within organizational or national boundaries, PQC requires a globally coordinated effort. A single weak link in the chain: a country, industry sector, or critical vendor that delays adoption could compromise the security of interconnected systems worldwide.
- **Proactive vs. Reactive Migration:** Previous transitions often occurred after a vulnerability was discovered (e.g., MD5 collisions, SHA-1 weaknesses). PQC migration is unique in that it is proactive. We are transitioning before quantum computers capable of breaking current cryptography become mainstream.

THE IMMATURITY OF A NASCENT CRYPTOGRAPHIC ECOSYSTEM

Despite NIST's standardization efforts, the PQC ecosystem remains profoundly immature compared to the decades-hardened RSA/ECC infrastructure:

- **Limited Cryptanalytic History:** RSA and ECC have endured 40+ years of intense scrutiny. The new PQC algorithms, while rigorously vetted, have only been studied for 10–15 years. History shows that new cryptography often reveals hidden vulnerabilities years later, meaning flaws remain a real risk.
- **Performance Characteristics as Unknown Variables:** Real-world performance of PQC algorithms at enterprise scale is not fully understood. While lab benchmarks exist, their behavior across varied hardware, network conditions, and combined protocols remains uncertain with larger key sizes being just one dimension of the unknown.
- **Implementation Pitfalls and Side-Channel Vulnerabilities:** Cryptographic history is full with examples of theoretically secure algorithms broken through implementation flaws, timing attacks, power analysis, or other side-channel vulnerabilities. The novel mathematical structures of PQC algorithms (lattices, hash-based constructions, etc.) introduce new implementation challenges that the security community is only beginning to understand and address.

THE INTEROPERABILITY CHALLENGE IN A FRAGMENTED WORLD

The global IT ecosystem represents perhaps the most complex system ever created by humans. It is a constantly evolving tapestry of hardware, software, protocols, and standards. Introducing new cryptographic primitives into this ecosystem creates profound interoperability challenges:

- **Protocol and Legacy Limitations:** Systems and standards like TLS, X.509, and HSMs have built-in size and performance limits. PQC's larger keys and signatures can exceed these, and legacy infrastructure, often embedded in critical systems for decades, may be impossible to upgrade.
- **The Hybrid Certificate Bridge and Its Complexity:** Hybrid certificates, which combine traditional and PQC algorithms, offer backward compatibility but double the complexity and cryptographic operations, creating new potential points of failure.

- **Vendor Adoption Asynchrony:** Vendors from chipmakers to cloud providers will adopt PQC at different speeds. This mismatch forces organizations to juggle multiple cryptographic configurations simultaneously, creating temporary incompatibilities.

Part 2 | A Lifecycle of Risk: Detailed Analysis of PQC Vulnerabilities Across PKI Stages

To understand the practical risks of PQC adoption, we must examine how they manifest across each stage of the Public Key Infrastructure lifecycle: The framework that manages digital certificates and public-key encryption.

DISCOVERY: THE INVISIBLE THREAT LANDSCAPE

Risk Deep Dive: Certificate discovery in modern enterprises is already challenging, with certificates often scattered across cloud instances, containers, IoT devices, embedded systems, and legacy hardware. The PQC transition introduces new classes of certificates (pure PQC, hybrid traditional/PQC) that existing discovery tools are not designed to recognize. These tools typically search for specific algorithms (RSA, ECC) or key sizes; they may completely miss PQC certificates using algorithms like Dilithium or Falcon.

Mitigation Strategy: Organizations must adopt discovery tools specifically designed for the PQC era. These tools should:

- Use multiple discovery methods: Network scanning, agent-based inventory, API integration with cloud providers, and integration with configuration management databases.
- Recognize all certificate formats, including those containing PQC algorithm identifiers (OIDs).
- Maintain an up-to-date database of PQC algorithms and their properties.
- Provide risk scoring based on algorithm type, key size, expiration date, and system criticality.

ISSUANCE: WHERE THEORY MEETS (AND BREAKS) REALITY

Risk Deep Dive: The issuance of the first PQC certificate in a production environment represents a critical inflection point. The larger key sizes and signatures of PQC algorithms create multiple potential failure points:

- **Protocol Limitations:** Many protocols have maximum sizes for cryptographic elements. For example, a TLS certificate chain with PQC signatures might exceed the maximum record size, causing handshake failures. Some implementations of protocols like SSH or IPsec have hard-coded buffer sizes that cannot accommodate larger PQC signatures.
- **Storage and Memory Constraints:** Hardware Security Modules (HSMs), smart cards, and embedded devices often have strict memory limitations. Storing PQC private keys (which can be larger than their traditional counterparts) or processing PQC operations may exceed these limits. Similarly, network devices like load balancers, firewalls, and WAN optimizers may have limitations on certificate sizes they can process.
- **Validation Pipeline Breakdown:** The certificate issuance workflow involves multiple systems: the certificate authority, validation services, and the requesting system. Each component in this pipeline must be upgraded to handle PQC. A failure at any point for instance, a validation service that cannot parse a CSR containing PQC algorithm identifiers blocks the entire issuance process.

Mitigation Strategy: A phased, test-driven approach is essential:

1. Begin with hybrid certificates in test environments, monitoring all system components for issues.
2. Conduct performance and stress testing at scale to identify bottlenecks.
3. Work closely with PKI and software vendors to understand their PQC roadmap and capabilities.
4. Develop fallback procedures in case PQC issuance fails, ensuring business continuity.

RENEWAL: THE AUTOMATION IMPERATIVE IN A SHORTER-LIVED WORLD

Risk Deep Dive: The cybersecurity industry is moving toward shorter certificate lifetimes to limit the impact of compromise and reduce the lifespan of issued certificates. The 90-day lifetime for TLS certificates is now standard, with CA/B moving to 47 days by 2029. This trend intersects dangerously with PQC complexity.

Automated certificate renewal using protocols like ACME (Automated Certificate Management Environment) has become essential for managing certificates at scale. However, if the renewal automation is not PQC-aware, it will fail to properly request, install, or configure certificates with PQC algorithms. The consequences of failed renewal are immediate and severe: service outages, broken authentication, and loss of encrypted communications.

Mitigation Strategy:

- Upgrade ACME clients and other automation tools to be algorithm-agnostic or explicitly PQC-aware.

- Implement monitoring that alerts on renewal failures with sufficient lead time for manual intervention.
- Consider staggered renewal schedules to avoid simultaneous renewal of large numbers of PQC certificates, which could overwhelm systems.
- Test renewal workflows end-to-end in environments that mirror production complexity.

ROTATION: THE CRYPTO-AGILITY IMPERATIVE

Risk Deep Dive: PQC migration is an ongoing process. Cryptographic algorithms have lifecycles: they are adopted, mature, show weaknesses, and are eventually deprecated. The risk is implementing PQC rigidly, embedding specific algorithms deeply into systems and policies. When replacement becomes necessary, organizations face costly "forklift upgrades," especially problematic in long-lifecycle systems like industrial controls, medical devices, or critical infrastructure.

Mitigation Strategy: Crypto-agility must become a core design principle:

- **Abstraction Layers:** Implement cryptographic abstraction layers that separate business logic from specific cryptographic implementations.
- **Algorithm Negotiation:** Support flexible algorithm negotiation in protocols, allowing systems to agree on the strongest mutually supported algorithm.
- **Dual Support Periods:** Maintain support for both old and new algorithms during transition periods.
- **Governance Framework:** Establish clear governance for algorithm lifecycle management, including criteria for deprecation and replacement.

Part 3 | Systemic Risks: The Broader PQC Challenge Landscape

Beyond the PKI lifecycle, organizations face strategic, systemic risks in their PQC transition.

ALGORITHM CONFIDENCE AND THE MOVING TARGET

The NIST standardization process, while rigorous, cannot guarantee permanent security. Organizations must:

- Monitor cryptographic research for developments related to their chosen PQC algorithms
- Participate in industry forums and information-sharing groups
- Maintain the flexibility to transition to alternative algorithms if necessary
- Consider algorithm diversity (using different PQC algorithms for different use cases) to mitigate the risk of a single algorithm failure

COMPLIANCE AND REGULATORY UNCERTAINTY

The regulatory landscape for PQC is evolving:

- **Standards Lag:** Regulatory standards (FIPS, Common Criteria, sector-specific regulations) will inevitably lag behind cryptographic developments.
- **Jurisdictional Variations:** Different countries may adopt different PQC standards or timelines, creating challenges for multinational organizations.
- **Audit Preparedness:** Organizations must document their PQC transition strategy and decisions for audit purposes, even in the absence of specific regulations.

THE HUMAN FACTOR: SKILLS GAP AND KNOWLEDGE DEFICIT

Perhaps the most underestimated risk is the human capital challenge:

- **Scarce Expertise:** Cryptographers with deep PQC knowledge are rare and in high demand.
- **Developer Education:** Application developers need training to use new PQC APIs correctly and avoid implementation pitfalls.
- **Operations Training:** Security and IT operations teams need to understand how to manage and troubleshoot PQC-enabled systems.
- **Executive Awareness:** Leadership must understand the strategic importance and resource requirements of the PQC transition.

Part 4 | Strategic Navigation: Tools and Approaches for a Successful Transition

Given this complex risk landscape, organizations need a structured approach to PQC migration. Specialized management tools and frameworks are not just helpful but essential.

THE ROLE OF ADVANCED PKI MANAGEMENT PLATFORMS

Modern PKI management platforms can serve as central nervous systems for the PQC transition by providing:

- **Unified Cryptographic Inventory:** Continuous discovery and inventory of all cryptographic assets across hybrid environments, with special attention to identifying PQC and hybrid certificates that might be missed by traditional tools.

- **Lifecycle Automation with Crypto-Agility:** Automated workflows for issuance, renewal, and revocation that are algorithm-agnostic, capable of handling both traditional and PQC certificates through the same interfaces.
- **Risk Analytics and Visualization:** Dashboards that map algorithm usage across the organization, highlight systems that are not PQC-ready, and visualize dependencies between systems and cryptographic implementations.
- **Policy Enforcement and Compliance:** Centralized policy management that can enforce cryptographic standards (e.g., "all new certificates must be hybrid Dilithium/RSA-2048") and generate audit-ready reports documenting compliance with organizational policies and regulatory requirements.
- **Vendor and Ecosystem Management:** Tracking vendor capabilities and roadmaps, highlighting potential interoperability issues before they affect production systems.

DEVELOPING A PHASED MIGRATION STRATEGY

A successful PQC transition follows a deliberate, phased approach:

1. **Inventory and Assessment (6-12 months):** Discover all cryptographic assets, assess their quantum vulnerability, and prioritize systems based on sensitivity and exposure.
2. **Laboratory Testing and Pilot (12-18 months):** Test PQC algorithms in isolated environments, evaluate performance impacts, and identify integration challenges.
3. **Controlled Production Deployment (18-36 months):** Begin deploying PQC in non-critical systems, using hybrid approaches where necessary, while monitoring performance and stability.
4. **Broad Production Deployment (24-48 months):** Expand PQC deployment to critical systems, maintaining backward compatibility during the transition.
5. **Optimization and Crypto-Agility (Ongoing):** Continuously monitor the cryptographic landscape, ready to transition to new algorithms as needed, maintaining crypto-agility as a permanent capability.

BUILDING ORGANIZATIONAL CRYPTO-AGILITY

Beyond technology, organizations must cultivate crypto-agility as an organizational capability:

- **Governance Structure:** Establish a cross-functional cryptographic governance committee with representation from security, IT, legal, and business units.
- **Education and Training:** Develop ongoing training programs for different roles within the organization.
- **Vendor Management Framework:** Create processes for evaluating vendor cryptographic capabilities and roadmaps.
- **Testing and Validation:** Maintain testing environments that can evaluate new cryptographic implementations before deployment.
- **Incident Response Planning:** Include cryptographic failures and transitions in incident response plans.

Conclusion: The Quantum Resilience Imperative

The transition to Post-Quantum Cryptography represents one of the most significant technical challenges the global digital ecosystem has ever faced. The risks are substantial, multifaceted, and span technical, operational, and strategic dimensions.

The organizations that will successfully navigate this transition are those that:

1. **Start now,** recognizing that this is a multi-year journey that cannot be rushed at the last minute.
2. **Adopt a crypto-agile mindset,** building systems and processes that can evolve as cryptography evolves.
3. **Implement comprehensive discovery and management tools** that provide visibility and control across their cryptographic landscape.
4. **Develop internal expertise** through training and strategic hiring.
5. **Engage with vendors, standards bodies, and industry groups** to stay informed and influence the direction of the transition.

Data encrypted now with traditional algorithms could be harvested and stored by adversaries for decryption when quantum computers arrive; A threat known as "harvest now, decrypt later." The time for planning and action is not when the quantum computer arrives, but now, while we still have the luxury of time to build resilience methodically and deliberately.

The cryptographic great migration has begun. The question is not whether organizations will make the journey, but how well-prepared they will be for the challenges along the way.

Munis Badar is the Founder & CEO of Securetron who has worked across multiple industries addressing complex security challenges over 20 years. He is a visionary leader with a passion for innovation and cybersecurity.

Converging Paths: Where Cyber Insurance and Security Intersect

by Jonathan Weekes, Presented by BOXX Insurance

2026 marks a turning point where the cyber insurance and cyber security sectors are converging into one shared ecosystem of resilience.

AI-driven attacks, increased regulatory scrutiny and accelerated digital transformation are reshaping how organizations perceive cyber risk and invest in their defenses. The shift is unmistakable: what was once viewed as a "tech problem" is now a systemic business risk with implications for governance, reputation and operational continuity.

By the end of 2025, businesses worldwide will have lost more than USD $10.5 trillion to cyber crime. It's a staggering figure that, if measured as a country's GDP, would rank cyber crime as the world's third-largest economy behind the United States and China. And it's only growing. The global cost of cyber crime will reach USD $13.8 trillion by 2028. In Canada, that number is expected to surpass USD $4.8 billion.

Already, Canadian organizations face an average breach cost of CAD $6.9 million, alongside a 24% rise in AI-enhanced phishing attacks, which have become the country's most common attack vector, according to IBM's latest Cost of a Data Breach Report.

As the threat landscape evolves, organizations are recognizing that managing cyber risk today demands integration, uniting technology, governance and financial protection.

Cyber insurers are stepping up, extending beyond reimbursement to become active participants in prevention, detection and recovery under one shared goal: Resilience.

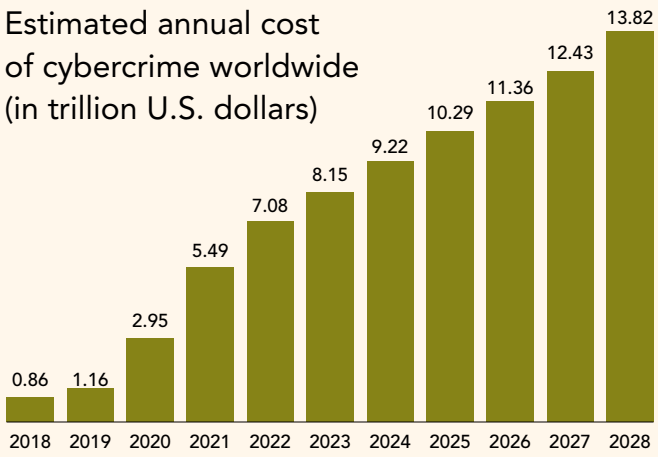
Insurance As Cyber Standard Setter

Insurance is moving from afterthought to ally. Historically, insurance policies were reactive, focused on covering financial damage and triggered only after an incident caused a loss.

Today, cyber insurers are co-designing cyber security standards, driving minimum control expectations across the market and rewarding clients for better cyber hygiene. Underwriting criteria now shape corporate security baselines, with boards increasingly viewing cyber insurance as a validation of organizational resilience rather than just a financial safety net.

For example, many cyber policies now require three of the most effective controls against cyber threats: Multi-Factor Authentication (MFA), endpoint detection and response (EDR) and incident response planning and testing, as well as encourage insurance clients to implement robust patch management. This approach is leading to closer collaboration between CISOs, risk managers, brokers and underwriters, shifting the industry towards proactive risk management.

Cybercrime Expected To Skyrocket



As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

87%

of Canadian organizations of all sizes experienced some form of cyber incident in the past 12 months.

Canada's Cyber Resilience and Maturity Gap

Despite growing awareness, recent research shows Canada's cyber security maturity and resilience gap leaves many organizations vulnerable to prolonged disruption. While overall attack volumes are declining, the number of successful cyber incidents remain steady as cyber attackers evolve their tactics to bypass security defences.

According to the CDW 2025 Canadian Cyber security Study, 87% of Canadian organizations of all sizes experienced some form of cyber incident in the past 12 months, including denial-of-service (DDoS), cloud compromise and data breach events. Even more concerning: the average downtime rose a significant 10%, reaching 14 days per incident.

Security maturity directly influences an organization's ability to prevent and recover from cyber incidents. The report found only 9% of Canadian organizations have achieved Strategic Security maturity — a fully automated, continuous approach that gradually improves posture. Most businesses remain reactive or inconsistent in security execution, limiting their detection, response and recovery capabilities.

For Small and Medium-sized Enterprises (SMEs), which often lack the in-house cyber security resources needed to withstand today's cyber attacks, the threat landscape is even more severe.

By the fall of 2025, more than half of Canadian SMEs had suffered at least one cyber incident, including phishing, malware, financial fraud, ransomware and DDoS attacks. Cloud-related incidents against SMEs climbed to 50%, up from 47% from the previous year.

Despite this, fewer than half of SMEs in Canada have implemented any form of cyber defence and only 12% carry dedicated cyber insurance, according to a BDC study commissioned by the Insurance Bureau of Canada.

The reality is, no single organization, regardless of its size, is immune to today's sophisticated threat environment and no one can fight it alone. Building true cyber resilience will require collaborative partnership models that integrate cyber security, insurance and managed response into a unified, prevention-first framework.

The Prevention-First Imperative

Across the industry, cyber insurance providers are shifting from "incident response" to "incident prevention."

Forward-thinking insurance carriers and cyber security firms are partnering to create cyber resilience ecosystems that combine risk scoring, threat intelligence, attack surface management, continuous monitoring and behavioural analytics. These proactive insurance models integrate prediction and prevention services into comprehensive coverage solutions that bolster organizations' cyber resilience holistically.

These prevention-first approaches are reshaping cyber insurance underwriting practices, where:

- Continuous monitoring is replacing static questionnaires.
- Proactive alerts and managed-threat services are reducing claims frequency.
- Real-time intervention prevents many losses before they occur.

In a prevention-first model, insurance validates resilience rather than merely funding recovery.

Our breach-response team, for example, is able to mitigate 80% of claims before they happen, demonstrating how pre-emptive engagement outperforms post-loss response.

In a prevention-first model, insurance validates resilience rather than merely funding recovery.

Bridging Two Worlds: Partnership Models That Strengthen Cyber Resilience

Partnerships between insurers, cyber security vendors and incident response teams are defining the next generation of digital resilience for organizations.

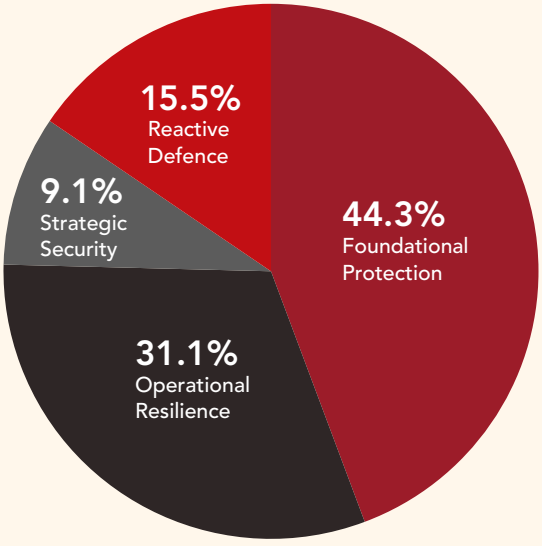
This integrated ecosystem approach replaces siloed models with collaborative frameworks that strengthen collective defence.

At their intersection, organizations co-develop detection and hygiene standards for:

- Sharing threat intelligence
- Establishing collaborative response playbooks that shorten containment times and reduce business downtime.
- Launching joint education programs and SME-focused outreach that raise cyber security literacy among businesses and individuals in Canada.

Insurance now becomes an operational partner, embedded within the systemic defence mechanism and no longer just a financial backstop. True cyber resilience depends on how effectively those who protect can help predict, prevent and recover.

Maturity of Canadian Cyber Security Programs



Source: CDW Canadian Cybersecurity Study 2025

A Stronger Cyber Ecosystem

Cyber security, insurance, regulators and businesses each hold a role in safeguarding Canada's digital economy.

When these sectors align their efforts, we'll see:

- Businesses gain earlier threat detection and faster recovery.
- The cyber insurance market stabilised through fewer, less severe claims.
- Standardized cyber controls gain wider adoption, raising the baseline of protection across industries.

This collaboration transforms cyber risk management from a series of isolated transactions into an interconnected ecosystem built on shared responsibility.

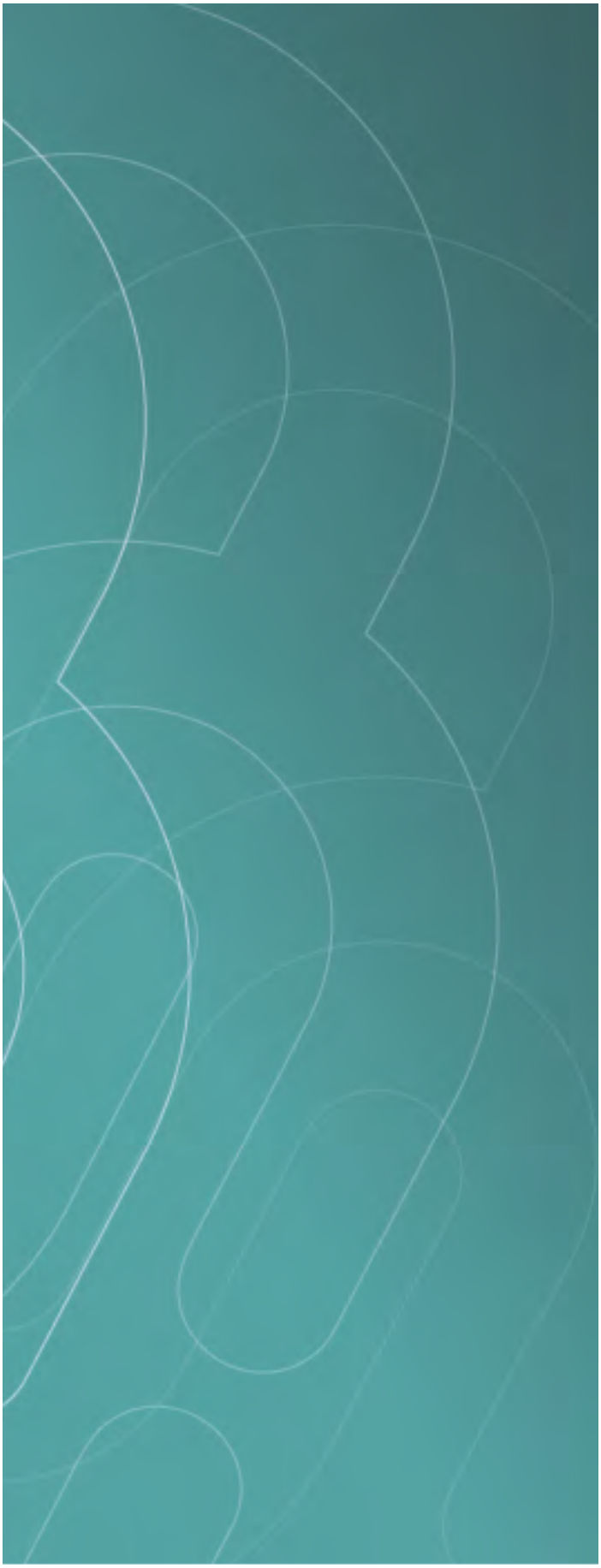
The Next Era of Cyber Resilience

The intersection between cyber security and insurance now defines the future of cyber resilience. Collaboration is reshaping expectations on both sides: policyholders demand greater value, and insurers require proven security practices. Mutual accountability is replacing transactional indemnity.

The next five years of Canada's cyber security maturity will be shaped by how organizations, insurers and technology partners align prevention with protection, supported by shared data, continuous validation and financial reinforcement.

The question is no longer whether cyber security and insurance can coexist, but how swiftly they can cooperate to make our digital world safer.

Jonathan Weekes is the President, Canada at BOXX Insurance and is a recognized expert in the field of commercial insurance, specializing in professional liability and cyber.



GIVE YOUR TEAMS THE ABILITY TO PREDICT & PREVENT

INCIDENTS BEFORE THEY ESCALATE

Cyberboxx® Assist is BOXX's prevention-first cyber services platform. Designed to help organizations detect threats early, reduce exposure, and intervene before incidents escalate.

Operating independently or with cyber insurance, it brings continuous monitoring, expert-led response, and proactive controls together into a single, scalable approach to organizational cyber resilience.

For program-level Cyberboxx® Assist deployments & partnerships, connect with:

Jonathan Weekes
President, Canada
BOXX Insurance
concierge@boxxinsurance.com

BOXX INSURANCE **PREDICT. PREVENT. INSURE.**

www.boxxinsurance.com

2025: The Year Cybersecurity Became a Systemic Resilience Mandate

by Femi Ogunji

The year 2025 will be remembered not just for the severity of cyber incidents but for the fundamental shift in regulatory and corporate philosophy that they necessitated. Before 2025, cybersecurity was often viewed through the lens of prevention—a defensive perimeter intended to repel all attacks. By the end of the year, that perspective had been permanently replaced by the doctrine of resilience, acknowledging that penetration is inevitable and that business survival hinges on rapid recovery. This mandatory pivot was the direct result of two parallel forces: the industrialization of cybercrime and the enforcement of groundbreaking legislation, such as the Digital Operational Resilience Act (DORA). The total economic damage caused by cybercrime worldwide, estimated at $10.5 trillion, confirmed that the threat was no longer a technical nuisance but a systemic risk to the global economy, as noted by Cybersecurity Ventures in its latest reports.

The Industrialized Threat Landscape

Cybercrime groups ceased operating as loosely organized hackers; in 2025, they fully embraced the model of the enterprise-grade adversary. These groups adopted mature business structures, including dedicated human resources, payment processors, and quality assurance processes, effectively turning Ransomware-as-a-Service (RaaS) into a highly efficient, multi-billion-dollar global industry.

QILIN AND THE VOLUME PLAY

The Qilin Ransomware Group epitomized the industrialization of volume and speed. Qilin's operational surge was unparalleled, executing 81 recorded attacks in a single month during the spring, representing nearly a 50% rise in activity, as documented by threat intelligence firm Group-IB. This was achieved not by creating revolutionary new malware, but by professionalizing their victim-identification and exploitation pipeline. Qilin focused on

maximizing the number of breaches through well-researched, automated methods, treating victim organizations not as isolated targets but as commodities in a high-volume market.

A significant, high-profile data theft from a major Swiss Bank later in the year demonstrated Qilin's appetite for high-value targets, showing that their volume strategy was matched by a precision targeting capability when needed. This approach, utilizing broad, rapid initial access followed by surgical, high-stakes data extraction, made them uniquely problematic, challenging defenders who were still focused on single-stage attack detection. The sheer volume of their activity forced organizations to rethink their priorities, shifting resources from trying to stop every attack to ensuring they could quickly detect and contain the one that inevitably got through.

The sheer volume of their activity forced organizations to rethink their priorities, shifting resources from trying to stop every attack to ensuring they could quickly detect and contain the one that inevitably got through.

CLOP AND THE STRATEGIC SUPPLY CHAIN STRIKE

In contrast to Qilin's volume-based strategy, the Clop ransomware group demonstrated mastery in strategic exploitation of shared software vulnerabilities. Clop's success in 2025 was primarily built on supply chain leverage. Their exploitation of a critical flaw in the widely used Oracle E-Business Suite caused a vulnerability with a severity score of 9.8, it was a masterstroke of precision. By compromising a single, critical piece of software used by numerous large enterprises for core functions like finance and logistics, Clop achieved widespread impact with minimal initial effort.

This supply chain attack model forces organizations to adopt a "trust nothing" approach, especially regarding third-party software and vendors. The incident served as a stark reminder that vulnerability management must extend beyond internally developed code to include rigorous, continuous auditing of third-party dependencies. If a piece of software is used by twenty major companies, exploiting its zero-day flaw effectively grants the attacker twenty breaches for the price of one discovery. Clop's work cemented the need for advanced behavioural detection, identifying the *anomalous activity* within a trusted application, rather than just the known signature of the attack itself.

The Persistent Human Element: A Vulnerability Analysis

Despite billions invested in firewalls and advanced defence tools, the year 2025 proved, yet again, that the human element remains the most potent and exploitable vulnerability. The technical sophistication of AI-powered defence often collapses under the weight of simple, yet perfectly executed, social engineering.

The high-profile DoorDash breach in late 2025 provides a textbook example of this failure. The attack was not initiated through a complex zero-day exploit but through a sophisticated impersonation. The attacker successfully posed as a trusted third-party vendor or partner, leveraging highly credible details obtained through reconnaissance to bypass standard human verification steps. Once initial access was granted through this deception, the attacker was able to navigate the internal network, gaining access to sensitive customer and internal data.

This incident underscores a crucial point for security leaders: perimeter defence is dead. The attack originated outside the technological defences, striking at the psychological layer. In response, organizations accelerated the adoption of comprehensive security awareness training, moving beyond annual slideshows to integrate real-time, personalized training modules that simulate current threat techniques. More importantly, the industry recognized the critical role of Extended Detection and Response (XDR) tools in this context. XDR is designed to detect the *consequences* of human error. It may not stop a user from clicking a malicious link, but it can immediately flag the subsequent anomalous activity, a user account logging in from an unusual location, accessing an abnormally large volume of data, or attempting to install unauthorized software. The DoorDash incident solidified XDR's role as the essential safety net for when the human firewall fails.

The Regulatory Hammer: DORA and the Mandate for Resilience

The massive financial losses and the systemic nature of the cyber threat provided the impetus for global regulators to intervene

with force. The most impactful regulatory event of the year was the enforcement of the European Union's Digital Operational Resilience Act (DORA), which became fully enforceable on January 17, 2025.

DORA is not just another compliance checkbox; it is a profound philosophical statement. It mandates that critical financial entities and their key ICT service providers must demonstrate their ability to withstand, respond to, and recover from all types of ICT-related disruptions and threats. As the European Parliament noted in its official DORA documentation, the act recognizes that "ICT-related incidents will inevitably occur." This paradigm shift moves the board-level discussion from "How do we prevent a breach?" to "How quickly can we resume critical business functions *during* a breach?"

This regulatory push immediately compelled organizations across all regulated industries to treat cybersecurity failures as operational risks, on par with market and credit risks. This forced boardrooms to allocate mandatory funding toward resilience components:

1. **Incident Response and Recovery Planning:** Detailed, tested, and audited playbooks for restoring data and systems within specified Recovery Time Objectives (RTOs).
2. **Threat-Led Penetration Testing:** The use of advanced testing methods that simulate the tactics of groups like Clop and Qilin.
3. **Third-Party Risk Management:** Stricter contractual requirements and deeper audit rights over critical cloud providers and IT service vendors.

DORA's influence extended far beyond the EU, establishing a global benchmark for operational resilience that other major economies began to adopt or emulate, creating a baseline expectation for cyber maturity worldwide.

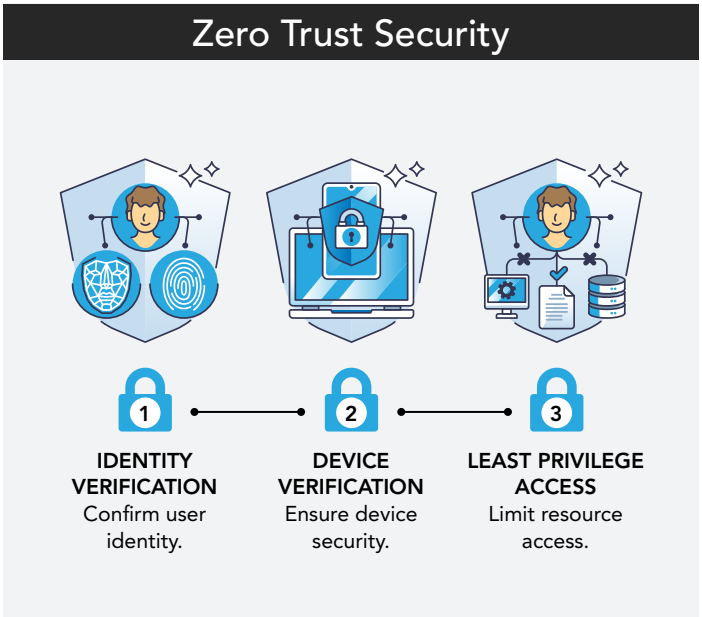
Architectural Evolution: Zero Trust and XDR Convergence

In response to the dead perimeter and new resilience mandates, security architecture underwent a definitive consolidation, centring on Zero Trust (ZT) as the foundation and Extended Detection and Response (XDR) as the operational engine.

ZERO TRUST AS THE DEFAULT

Zero Trust moved from a theoretical concept to the default, non-negotiable architectural model for modern enterprises. Driven by the permanence of hybrid work, the ubiquitous use of cloud services, and the proliferation of IoT devices, the traditional network boundary vanished. As analysts at Forrester Research predicted, the question was no longer *if* ZT should be adopted, but *how* it should be rigorously implemented across every component of the IT estate.

Implementing Zero Trust involves more than just micro-segmentation; it requires a deep investment in identity management and contextual access control. Every user, device, and application attempting to access a resource must be continuously verified,



authorized, and limited to the minimum necessary permissions (Principle of Least Privilege). The implementation challenges in 2025 centred on managing ZT across sprawling multi-cloud environments, ensuring policy consistency across AWS, Azure, and Google Cloud, and integrating it with legacy on-premises infrastructure. Successful implementation required robust API integration, automated provisioning, and tools that enforce policy based on real-time factors such as device health, location, and the sensitivity of the requested resource.

THE XDR UNIFICATION

Simultaneously, the industry embraced XDR as the answer to the chaos of siloed security tools. Before 2025, security operations centers (SOCs) were often drowning in alerts from disparate systems: one for endpoints (EDR), one for email, one for the cloud, and one for identity. XDR addresses this inefficiency by unifying the data lake and correlation engine across these critical security telemetry points.

This unification allows security analysts to see the full narrative of an attack—from the phishing email (email telemetry) that

granted the initial access, to the lateral movement (endpoint telemetry), and finally to the data exfiltration attempt (cloud or identity telemetry). The net result is a massive reduction in the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). By consolidating tools and leveraging machine learning for cross-platform correlation, XDR platforms allow human analysts to focus on high-fidelity threats, thereby mitigating alert fatigue and improving the efficiency of scarce security talent, a point highlighted by Gartner in their 2025 security operations reports.

An Eye to the Horizon: Post-Quantum Cryptography (PQC)

While the focus of 2025 was on immediate threats and resilience, a critical success story was the move toward long-term threat mitigation: the strategic adoption planning for Post-Quantum Cryptography (PQC). Although true quantum computing capable of breaking current encryption is still years away, the timeline for transitioning global infrastructure is decades long, leading to the concept of "Harvest Now, Decrypt Later." Threat actors are already harvesting encrypted data today, intending to store it until quantum capabilities mature.

The United States National Institute of Standards and Technology (NIST) continued to finalize its selection of quantum-resistant cryptographic algorithms, prompting large technology firms and government agencies to initiate comprehensive cryptographic inventories. This proactive approach—identifying all encrypted assets and creating detailed migration roadmaps—was essential. PQC planning, while not stopping 2025's ransomware attacks, represents the most significant investment in long-term data security, signalling a new level of maturity in corporate risk governance.

Conclusion: The New Mandate

2025 closed the chapter on perimeter-centric, purely preventative cybersecurity. The overwhelming evidence from industrialized threat groups like Qilin and Clop, coupled with the systemic risk highlighted by the DoorDash failure, solidified the necessity of the resilience mindset. Backed by the legal force of DORA, organizations must now demonstrably prove their ability to recover and continue operations during a cyber event. The successful adoption of Zero Trust and XDR provided the necessary architectural and operational tools to manage this new reality. For security professionals, the mandate is clear: the most valued skill is not just stopping an attack, but engineering a system that is fundamentally unbreakable in its ability to persist critical functions.

See end notes for this article's references.

Femi Ogunji is a Senior Security Consultant who brings 17+ years of experience in technology, with the last 9 years dedicated to cybersecurity, spanning advisory, risk management, and strategic security initiatives.

CCN INSIGHTS

Executive Briefings on Cybersecurity and Digital Risk

Executive insight for leaders evaluating cybersecurity and digital risk.

CANADIANCYBERSECURITYNETWORK.COM/
CCN-INSIGHTS

Sponsor yours today.

ccn

Securing Critical Infrastructure: Canada Can Light the Way Forward

by Cheryl Biswas

2025 has been a year of disruptive challenges and seismic changes globally, affecting international relations, the economy, and the environment. The new year will need to find its way forward through missing landmarks and unfamiliar terrain. International relations are strained and volatile against a backdrop of economic instability. Climate change has contributed significantly to the escalation in frequency and severity of natural disasters. Increased adversarial targeting and security incidents have negatively impacted critical infrastructure: power, water, communications, healthcare, transportation and more. These unexpected and unplanned-for challenges require Canada to rapidly acknowledge, respond, mitigate and defend for safety, and change course from existing strategies in economics, geopolitics and security to ensure the nation's digital sovereignty and endurance for the future.

Prime Minister Carney has presented an ambitious plan forward that emphasizes Canada's strengths in natural resources, rare minerals, technology and AI as the country pursues new global trade opportunities and self-reliance. Canada will need to leverage its substantial reserves of diplomatic goodwill to strengthen existing relationships and forge new ones while building a highly skilled workforce that develops and delivers on the advantages of emerging tech that expands reciprocal opportunities for growth. All of this requires reliable, vast quantities of power and energy, communications and Internet, transportation, water, and more, essential for Canada's road forward in new datacenters, pipelines, and economic initiatives. Critical infrastructure is essential to our survival and underpins all that we need to do and aspire to.

Adversaries will actively target and exploit any cybersecurity weaknesses for disruption or destruction, but they are not the only threat. Anything that causes the widespread loss of power, impairs communications, or prevents access to the multitude of online systems daily life relies on, presents a societal problem

Canada can light the way toward global collaboration and resilience.

with global impact. Therefore resilience must meet the challenge of change and navigating evolving threats in this new world order, because the reality is that there will be damage with increasing potential for catastrophic levels. As cyberattacks and climate events become greater than any one nation can manage on their own, mitigation and recovery will require resilience powered by community and collaboration. As the saying goes "If you want to go fast, go alone. If you want to go far, go together." Through its domestic security initiatives and diplomatic strengths, Canada can light the way toward global collaboration and resilience.

Critical Infrastructure in Canada

Critical infrastructure is that infrastructure governments deem essential for the economy and society to function, and as such it deserves special protection because of its importance to national security, and the high value target it presents to adversaries. Each country determines what sectors comprise their critical infrastructure. In Canada those ten sectors are: Energy/ Utilities; Manufacturing; Health; Government; Transportation; Information and Communications; Finance; Food; Water; Safety. These sectors directly contribute to the collective safety and stability of Canadian society, connecting a vast territorial landscape with remote, sparsely populated regions, and enabling technological advancements and economic growth that provide jobs, education, and social benefits. Prime Minister Carney established his mandate to "build Canada strong" in his first federal budget released in November 2025, shifting from reliance to resilience and protecting Canada's sovereignty and security while building a stronger Canadian economy. As Canada builds forward in this new strategic initiative to position itself in the development of emerging tech and AI, these new datacenters are critical infrastructure that relies on other critical infrastructure. As the country seeks to increase the economic benefits of oil and gas reserves, pipelines take on new significance. The ambitious road forward emphasizes digital sovereignty and digital infrastructure, but these are dependent on the security and reliability of the physical and critical infrastructure on which they ride.

Threats

It is essential to understand that the predominant technology used in critical infrastructure is Operational Technology (OT) and differs from Information Technology (IT) in that OT prioritizes availability (uptime) and systems integrity, whereas IT prioritizes confidentiality and data integrity. Where once there were sizable defensive gaps, critical infrastructure is increasingly linked to and exposed by IT systems. Securing IT does not adequately secure OT, however exploited IT systems enable the compromise of adjacent OT. To effectively secure infrastructure, it is necessary to understand a big picture view of threats against both IT and OT systems

STATE-SPONSORED ADVERSARIES

State-sponsored adversaries are highly skilled, highly resources threat actors, and most are attributed to China, Russia, Iran or North Korea. Over recent years, lines have blurred and it is imperative to factor in their support and relationships with hacktivists and ransomware gangs as dangerous proxies, as seen through targeted cyber attacks against transportation, water systems, government, finance, and energy. As major technology and cybersecurity companies have cut skilled workforces, there have been ongoing discoveries of state-sponsored actors dwelling within critical communications infrastructure for months to years. Adversaries will identify and exploit systemic vulnerabilities just as they do technical vulnerabilities for access and control.

Russia is known for targeting critical infrastructure in destructive attacks. One of their most dangerous groups, "Sandworm," took down Ukraine's power grid in December 2015 in a cyberattack that created physical damage. Since at least 2021, the group has actively been targeting energy, oil and gas, telecommunications, shipping, and defense/arms manufacturing sectors and has deployed destructive wiper malware. Per Jodi Summer Williams on LinkedIn, Senior UK defence and intelligence leaders, including Sir Richard Knighton, Chief of Defence Staff and Blaise Metreweli, MI6 Chief, have recently issued warnings about increased Russian cyberattacks and sabotage against UK critical infrastructure. But this warning applies globally.

Sabotage is becoming more subtle, frequent, and deniable through the use of proxies. In his November 13, 2025 address, CSIS Director Dan Rogers made clear that Canada is becoming a more active target. When fiber cuts happen, a team of two people can require 8-12 hours for full repair, at a potential cost of at least $15,000 for a single 144-count cable. Undersea cable restoration is even more dire, with only a handful of ships ready to deploy that are equipped with the people and resources required.

China has posed a longstanding threat to critical infrastructure through their attacks on U.S. networks, including water and power systems. Cybercommand General Tim Haugh warned on a 60 Minutes episode that China was seeking to "gain the advantage in an upcoming attack" by hacking Americans in their homes. In February 2024, CISA warned that PRC state-sponsored threat actors sought to pre-position themselves on IT networks for disruptive or destructive cyber attacks against U.S. critical infrastructure in the event of a major crisis or conflict with the U.S. The threat group Volt Typhoon is believed to be used to "cause disruption and sow societal panic." Chinese interference and espionage campaigns against Canada have been identified, and the full extent of their compromise and intent is likely underestimated.

CENTRALIZATION

Over the past several years, many business productivity platforms rely on just a few Software as a Service (SaaS) vendors. Industries rely on critical lines of business applications from these same vendors, which are hosted on one of the major clouds – Google, AWS, Microsoft – without multi-cloud redundancy. When AWS (U.S.-EAST-1) suffered a major outage in October 2025, the impact to business as well as consumers was immediate and enormous. Downtime, and increased interdependency, come with serious hidden costs. The Internet was not designed to become the load-bearing critical infrastructure for everything that it now is.

WEATHER AND NATURAL DISASTERS

We live in a world where the increased risk of natural disasters impacting critical infrastructure and technology result in unpredicted and uncontrollable consequences. Telecommunications networks are often the first to go down during a disaster. Electrical grids are highly interdependent, so when one goes down, they all may go down. That leaves us without communications when we most need it to get the word out, call for help, coordinate safety and rescue.

When surface infrastructure like roads and bridges are wiped out, rescue crews cannot reach survivors in time or deliver emergency supplies where they are needed The Government of Canada has mandated that citizens are responsible to ensure they have sufficient food, water and supplies for the first 72 hours of an emergency. What if you can't shelter in a place where you have access to your belongings? How do you help people to be prepared with gas, water, medicines if they need to evacuate immediately?

The reality is that climate change continues to increase the frequency and severity of natural disasters, resulting in devastating impact and loss. The risk to critical infrastructure from natural threats also creates opportunities for adversaries to exploit moments of disruption. This is not just about the risk of damage to critical infrastructure we rely on daily, but the opportunity for adversaries to weaponize that. This has been demonstrated by online scams and fraud by cyber criminals leveraging public sympathy and monetary support in response to disasters. Panic, fear, desperation – what are the playbooks for societal breakdown?

The risk to critical infrastructure from natural threats also creates opportunities for adversaries to exploit moments of disruption.

RISKS FROM GEOPOLITICAL DEPENDENCIES AND SHIFTS

2025 witnessed the dismantling of major U.S. government agencies following the 2024 presidential election. Massive reductions in workforce for cost cuts resulted in the "hollowing out" of CISA and monitoring agencies, creating long-term loss in capability and defensive posture, a loss that is hard to rebuild. Unfortunately, this opens up the U.S. and all the external dependencies that relied on these capabilities and services to massive exposure and long-term vulnerability. It is likely to get worse as the new U.S. National Security Strategy pulls the U.S. out of their responsibilities in the global arena.

DATA SOVEREIGNTY

At the speed of technology development in a world driven by data, when geopolitical shifts come with seismic impact data sovereignty

now plays a crucial role in national security, resilience and protecting critical infrastructure. For Canada, this means understanding that per the U.S. Cloud Act, hosting data in Canada does not keep the data from American authorities. U.S. law enforcement can compel a U.S. company, through their Canadian subsidiary, to comply and hand over data without no requirement to notify the data owner. Data residency does not ensure data sovereignty, and the contents and control over that data can impact the operation and integrity of critical infrastructure systems. This impacts Canada's plans for AI and datacenter innovation given that the major cloud providers – AWS, Google, Microsoft – are U.S. based so that data is subject to foreign jurisdiction.

Resilience

Recover, restore, withstand, adapt. Resilience was mentioned multiple times in The State of Cybersecurity 2025 report. Deryck Greer gave an excellent assessment:

> 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.

The responsibility is collective, and rests with individuals, organizations, and governments. This will be driven by coordination, community, and collaboration.

SOCIETAL IMPACT

Modern society is organized, built on communication, governance, and shared culture. Technology provides the tools to develop infrastructure for abundant food, specialized labour, stable communities, social order, and the long-term continuity of people. In the Wired For Change Podcast "Canada Under Pressure: Navigating the Hybrid Threat Landscape," Lina Dabit stressed the need to pay attention to the big picture while listening to what's happening on the ground, to move past silo thinking and look for what has not been accounted for. These technological developments come with increased interdependency, which leads to cascading risks so that small disruptions have significant downstream impacts as when the power supply goes down, and brings down everything with it. How are we planning for increased disruptions and more destructive cyber attacks? How are we adjusting preparations for when specific sectors go down to when combined sectors go down? For prolonged periods? The way forward required a "whole of system approach" when securing, and a whole of society effort to make that happen.

Canada's Initiatives

The road ahead requires commitment and leadership at all levels, especially within the relationships between private and public sector. The Government has key roles to play through policy and legislation that will establish standards for compliance, regulation, and enforcement. Bill C-26 initially addressed securing critical infrastructure and set obligations for telecommunications providers, finance, energy, and transportation. Canada is now waiting for the Critical Cyber Systems Protection Act, part of Bill C-8 which replaces C-26, to be passed to provide a national framework securing IT systems. In the new National Budget, Canada has committed to integrating cybersecurity into national security and digital sovereignty goals, providing significant funding for defence, AI, critical infrastructure protection, and a new National Cyber Security Strategy (NCSS) that focuses on a "whole of society engagement," developing talent, investing in AI and Quantum tech to increase domestic cyber capacity, and the Cyber Security Cooperation Program. This all hinges on the will to commit, because as shared by CISO Priscilla Kosseim on LinkedIn "The real challenge is not implementation, it is interpretation. Regulation creates structure, not resilience." In the end, it will only be as effective as we choose to make it.

Lina Dabit called out the role of community to build resilience and fill gaps, and how communities encourage people to look out for and look after each other, for collective safety. She has been passionate about helping to build resilience for Canada through public-private partnership, and finding resources within education and the public sector. Her key messages were to prepare people to succeed by knowing the plan and its contingencies, then effectively communicating roles and responsibilities. Ensure that collaboration is authentic, that what is said aligns with what must be done.

COMMUNITY ORGANIZATIONS

As critical infrastructure faces increasing threats at multiple levels, backup networks, out-of-band provisioning, and human connections are the investments to be made now to provide resilience when the grid is done. Grassroots movements and community efforts to establish and empower local cybersecurity capabilities become force multipliers for national cybersecurity, sharing the load of responsibility and enhancing visibility. The BC Cyber Hub Pilot Project: Strengthening Cybersecurity Resilience presents how regional hubs, or cybersecurity communities of practice, share the skills and experience of those with more cybersecurity maturity with those who are less mature, thus evening out the balance and reducing cyber risk nationally. Examples in the U.S. include the DEF CON Franklin initiative and UnDisruptable 27, with a focus on protecting water systems.

PREVENTING VULNERABILITIES AND MISHAPS

2025 has been a year of major cutbacks and workforce reductions, on the heels of massive reductions in prior years. Private organizations and entities must focus on their accountability to provide adequate resources to ensure enough skilled people are available to do the jobs that can never fully be automated or delegated to AI; to invest in training and maintaining employees so that burnout and exhaustion do not become the underlying causes of misconfigurations or missed warning signs.

DATA SOVEREIGNTY

The time is now for federal funding to build a sovereign Canadian cloud, with Canadian-owned infrastructure, and move beyond protecting individual privacy rights to addressing jurisdictional concerns. To foster the culture shift necessary to respond to the recent and rapid geopolitical changes, governments can encourage and reward companies to do their part in helping to establish and maintain data sovereignty, keeping Canadian IP on Canadian-owned infrastructure that cannot default into U.S. legal reach. There is tremendous business opportunity and reward for homegrown made in Canada initiatives here.

INTERNATIONAL RELATIONSHIPS

The importance of collaboration and cooperation for collective defence cannot be overstated. As has been demonstrated through multiple engagement, international collaboration between law enforcement agencies has been highly successful at taking down major dark web and cybercriminal operations which individual efforts simply could not. This same concept can be applied to multinational forums and relationships to secure critical infrastructure and resiliency.

Canada recognizes cyber risks and threats as international in scope and which require an international response. Canada is an advocate for the "Framework of Responsible State Behaviour in Cyberspace," which is a voluntary framework of behaviour developed across years of work at the UN to ensure international stability in cyberspace. Canada is well-positioned to leverage existing strong alliances and multilateral arrangements to strengthen its own cyber defenses and help build global cyber resilience as a member of the G7, NATO, UN, and more. As part of the Organization of American States (OAS), Canada engages in building regional cyber capacity. Within the G7, Canada helps lead initiatives like the Rapid Response Mechanism to detect and thwart foreign cyber interference. As the U.S. pulls back from its global roles, Canada can use this as the opportunity to step up its ongoing involvement and leadership globally, to build collective capability for detecting breaches, countering disinformation campaigns, and mitigating foreign interference. In his paper, "Firewalls and Frontlines: Canada's Cybersecurity Leadership Potential in the Age of Foreign Information Operations," David Dubé presents recommendations on how Canada can leverage its distinct advantages for leadership within the international community, but only once Canada has worked on secure digital identity systems and hardened itself to be less susceptible to foreign interference and disinformation campaigns, and implemented the necessary legislation for AI governance and securing telecommunications.

The time is now for federal funding to build a sovereign Canadian cloud with Canadian-owned infrastructure.

Conclusion

As technological advancement, geopolitical shifts, and climate change events evolve beyond expectations, organizations, public and private, must rapidly respond and change course from existing strategies to ensure Canada's digital sovereignty, societal stability, and economic endurance for the future. Individual nations need to ensure national resilience engaging the whole of society in the mission. Canada must develop domestic strategies that help safeguard critical infrastructure and resilience powered by community and collaboration. What lies ahead in this volatile and technologically evolving threat landscape also requires a trust network of strong external relationships to create a larger community for resilience, recovery, and support. Canada has the opportunity now to step up, to lead by example, and to foster global cooperation and collaboration for societal security and resilience.

See end notes for this article's references.

Cheryl Biswas is an independent cybersecurity analyst, experienced in strategic threat intelligence, tracking trends and emerging threats, and advocating for defending critical infrastructure. Her past experience includes employment with TD Bank, KPMG, CP Rail, and businesses in managed services, urban planning, architecture, and retail.

AI Cybersecurity and Trust in Canada Report Coming in April

Sponsor today.

CANADIANCYBERSECURITYNETWORK.COM/HUBFS/REPORTS

ccn

It Was Bad in 2018 — It's Worse Now

by Scott Augenbaum

When I retired from the Federal Bureau of Investigation (FBI) in 2018 after nearly three decades of service, I believed I had seen the worst of cybercrime. I had interviewed thousands of victims, and watched businesses lose millions overnight to scams that could've been stopped with one phone call. Back then, I warned individuals and organizations about phishing emails and ransomware. According to Cybersecurity Ventures, cybercrime was already a $3 trillion global problem. It was projected to double to $6 trillion by 2021. Fast forward to 2026 and the damage is staggering. Cybersecurity Ventures estimates cybercrime will cost the world over $15 trillion annually, making it one of the largest global economies if measured that way. Meanwhile, here in the U.S., the FBI's IC3 report shows $16.6 billion in reported losses in 2024 alone. But take it from me: after decades with the FBI, I can tell you that reported losses are just the tip of the iceberg. From my experience most victims never come forward because they're ashamed, afraid, or don't even realize they've been scammed.

Meanwhile, the tools used to carry out these attacks are getting cheaper, faster, and more convincing. Cybercriminals now operate like Fortune 500 companies. They have call centers. They use automation. They hire developers and analysts. The worst part? Most of this crime is entirely preventable. That's why I created the Cybersecure Mindset, a platform, a framework, and most importantly, a way of thinking. Because cybersecurity isn't a product. It's a mindset.

Victim Story: When "The Voice" on the Phone Wasn't Real

Let me share a real story I use in my training sessions. We'll call him Robert. Robert is a smart guy. CEO of a midsize company. Disciplined. Cautious. The kind of person most people think doesn't get scammed. One afternoon, he was attending his daughter's high school graduation when he got a call from his CFO. Her voice was tense.

> "Bob, there's a problem with a wire transfer. The client's bank just sent a stop-payment. We need to reroute the funds to a different account. I'm sending it to your phone now."

Robert didn't hesitate. The call came from her number. It sounded exactly like her. She even used their internal vendor nickname. He authorized the $450,000 wire transfer from his phone in under a minute. Except it wasn't her. It was a deepfake. An AI-generated voice clone, trained off a few minutes of public video from a speaking event. No hack. No technical breach. No ransomware. Just a fake voice and a moment of misplaced trust. The cybercriminals didn't break into Robert's company, they broke into his brain.

This is what I teach through the Cybersecure Mindset. Today's scams aren't about malware, they're about manipulation. If you don't understand how these criminals think, you'll never see it coming. That's why our best defense in 2026 isn't technology, it's awareness.

The Four Truths of Cybersecurity (Still True in 2026)

Over time, after hearing story after story like Roberts', I realized we were fighting the wrong battle. It wasn't just about stopping criminals, it was about changing how people think. That's what led me to discover four truths about cybercrime. These weren't written in some FBI handbook, they were carved from years of real conversations with victims. And they haven't changed even as the tools and tactics have.

TRUTH #1: NOBODY EXPECTS TO BE A VICTIM

Every victim I met said the same thing: "I never thought it would happen to me." That mindset; that this won't happen to me is exactly what criminals count on. I remember speaking with a retired teacher. Smart, thoughtful, cautious. She got an email from what looked like her bank. Same logo, same tone, even her full name. It asked her to verify a charge. She clicked the link and entered her info. That one click cost her everything.

TRUTH #2: ONCE THE MONEY'S GONE, IT'S GONE

This is the one nobody wants to hear and it's the hardest to accept. Once your money is in the hands of cybercriminals, it's almost always unrecoverable. They move fast, convert it to crypto, and route it through unreachable countries. I worked with a small business owner who lost a million dollars after wiring funds to what he thought was a known vendor. By the time he called his bank, the money was long gone, and the FBI had no jurisdiction where it landed.

TRUTH #3: BRINGING CYBERCRIMINALS TO JUSTICE IS JUST PLAIN HARD

Here's the reality: most cybercriminals aren't hiding in a basement in your town. They're overseas in places like Russia, China, Iran, North Korea, West Africa, and parts of East Asia. And while the FBI, U.S. Secret Service and RCMP do an outstanding job pursuing these cases, the truth is, bringing these criminals to justice is just plain hard. We're dealing with international boundaries, conflicting laws, and limited jurisdiction. Many foreign governments don't care especially when their own citizens aren't the ones being targeted. I know it's a tough pill to swallow. But with conflict happening around the world, it's getting even harder. We can't rely on the cavalry to show up after the fact. Prevention isn't just the best option sometimes, it's the only one.

If you had asked me in 1995 when I was a young FBI agent what the job was all about, I would've told you it was simple: Bad people did bad things to good people. We caught them. We put them in jail. It was exciting, fulfilling, and straightforward. The harder I worked, the more criminals I helped lock up. The better I felt. So, when I got into cybercrime investigations in the early 2000s, I figured it would be the same. How hard could it be? Follow the money. Trace the IP address. Knock on a door. Arrest the bad guy. Simple. Except it wasn't.

> The victims I met weren't careless. They were smart, responsible, and thoughtful. But they never expected to be targeted. And by the time they came to me, their money was already gone.

Worse, some of them were angry at me, I was the FBI, and I couldn't fix it. That stuck with me. One day, I sat with a man who had just lost over $600,000 in a scam. His family was devastated. In their grief and frustration, they looked at me and asked, "Why can't you help us as our dad lost everything?" And that's when it hit me. If he had just done a few small things differently, he wouldn't have been a victim at all. That was my turning point. That's when I realized the real answer wasn't just law enforcement, it was mindset. That moment inspired everything I teach today.

TRUTH #4: MOST CYBERCRIME CAN BE PREVENTED

This is the most important truth of all: Most cybercrime is preventable. It's not about technical skills. It's about habits and small behaviors that make a big difference. From my experience both during the FBI years and in the thousands of victim interviews I've done since, I estimate that 90% of cybercrime could be stopped with just a few consistent actions. These aren't tips. They're defenses. And in 2026, with scams evolving faster than ever, you need to think this way every day. The hard truth? Technology isn't the biggest vulnerability. We are.

The Intersection: Artificial Intelligence + Social Engineering = Explosive Growth in Cybercrime

If I had to name one force that has supercharged cybercrime in 2026, it's the collision of artificial intelligence and social engineering. Back in 1995, we didn't use the word cybercrime. But we saw the beginnings of scammers using phones, letters, and faxes to trick people out of money. We called it wire fraud or mail fraud. The methods were low-tech, but highly effective. And that's what social engineering is: Tricking people into doing something they normally wouldn't by preying on their trust, urgency, or emotions. The psychology hasn't changed but the tools have.

Now, thanks to AI, social engineering is faster, cheaper, and more convincing than ever. AI scrapes your data, mimics your voice, writes realistic messages, and automates entire scams. Criminals can launch attacks at a scale we've never seen and for almost no cost. They don't need to "hack" your system. They just need you to trust the wrong message, click the wrong link, or believe the wrong voice. Here's how that shows up in 2026 and how AI makes each attack stronger, faster, and more convincing:

EMAIL (PHISHING)

An executive assistant received an email from "HR" about urgent open enrollment deadlines. It included her full name, department, and an internal document link. She clicked — and unknowingly gave away her Microsoft login.

How AI makes it worse:
AI tools scrape public data on LinkedIn, company websites, press releases and generate perfectly written, personalized phishing emails that sound exactly like real coworkers or supervisors.

Lesson:
If an email feels urgent or out of place, slow down. Verify it through another channel — like a phone call or secure messaging.

TEXT MESSAGING (SMISHING)

An employee received a text from "the IT helpdesk" saying his VPN access was being revoked and to click a link to verify credentials. He did and handed them over.

How AI makes it worse:
AI can now generate thousands of smishing messages that are tailored with breach data, phone numbers, location, and workplace lingo — making fake texts feel authentic.

Lesson:
Never trust a clickable link in a text you didn't ask for. Open your VPN or corporate apps directly, not through links.

PHONE CALLS (VISHING AND DEEPFAKE VOICE)

A finance manager got a call from his "CEO" while the real one was traveling. The voice said to expedite a wire transfer and used project code names from past emails. It wasn't the CEO — it was a deepfake.

How AI makes it worse:
With as little as 30 seconds of online audio, AI voice cloning tools can replicate a colleague's voice with stunning accuracy and combine it with spoofed caller ID for extra believability.

Lesson:
Always confirm sensitive requests like wires or login resets through a known method. If it feels urgent and emotional, slow down

QR CODE PHISHING (QUISHING)

An office manager scanned a QR code on a flyer in the lobby labeled "New Remote Work Policy." It led to a fake Microsoft login page where she entered her password.

How AI makes it worse:
AI tools now create QR codes that direct users to fake login pages indistinguishable from real ones and can track which employees scan them, targeting them with follow-ups.

Lesson:
Don't scan QR codes from untrusted or public sources. Go directly to known URLs instead.

SOCIAL MEDIA ACCOUNT HIJACKING

A company's marketing manager had her LinkedIn hijacked. "She" began messaging vendors and clients about updated payment terms. Several wired funds went to the wrong place.

How AI makes it worse:
After hijacking an account, AI can mimic your tone, style, grammar, and even emojis keeping up realistic conversations before executing a scam.

Lesson:
Use MFA on every business-facing social platform. If a message from a colleague feels off, confirm through another source.

BUSINESS EMAIL COMPROMISE (BEC)

A bookkeeper got an invoice from her CFO's "email," referencing a real vendor and using phrases like "last quarter's drop." She wired $88,000 straight to a scammer's account.

How AI makes it worse:
AI can scan stolen email threads and generate perfectly phrased responses in your company's tone, referencing real past communications.

Lesson:
Never authorize wire transfers from email alone. Always use a secondary verification method like a phone call or secure messaging.

ROMANCE AND PIG BUTCHERING SCAMS (CRYPTO FRAUD)

A professional met someone on a dating app. She claimed to be in finance and slowly pulled him into a crypto investment opportunity. He lost $240,000 to a fake platform.

How AI makes it worse:
AI-powered bots carry on long, emotionally manipulative conversations over weeks or months. Deepfake video calls and fake trading dashboards complete the illusion.

Lesson:
Romance and investing don't mix. If someone you haven't met in real life is talking about money, stop.

POP-UPS AND FAKE TECH SUPPORT

An employee's screen froze during a Zoom call, showing a system error and a "Microsoft support" number. He called it and gave remote access to his work device.

How AI makes it worse:
AI now designs realistic pop-ups that mimic Windows and macOS down to the fonts, error sounds, and fake diagnostics complete with fake support lines staffed by scammers.

Lesson:
Never call numbers that appear in pop-ups. Restart the device or report it to your real IT team.

LOOK-ALIKE DOMAINS

An HR manager searched for "ADP login" on Google and clicked the top result — which was a fake domain like adp-payroll-login[.]com. Her credentials were harvested instantly.

How AI makes it worse:
AI generates thousands of typo-squatting domains and perfectly cloned login pages, then boosts them through search ads or SEO manipulation.

Lesson:
Don't trust search engines for login pages. Type the address directly or use your company's official links.

In 2026, cybercriminals don't need to break into your systems. They let AI do the recon and count on your brain to do the rest.

2026 Reality: The Data Breach Is Already Inside Your House

Here's the harsh truth: your data is already on the dark web. Billions of usernames, passwords, and personal info have been exposed in recent breaches. Every time a trusted site like LinkedIn, Dropbox, Facebook and many others are breached, your data ends up for sale. And cybercriminals use that stolen data to break into your accounts without hacking anything.

It's called credential stuffing: They try your old usernames and passwords on your bank, your email, your cloud storage and if you reuse passwords, they're in. You're not being hacked. You're being logged into. This is where mindset matters most.

Let me tell you about Ray. Ray owns a successful business. Smart. Cautious. But like many people, he never set up multi-factor authentication (MFA) on his email. One day,

a cybercriminal logged in using an old password from a breach years ago. From there, they read through Ray's inbox and learned everything about him, where he banked, how he handled wire transfers and his cell phone provider. Then, they took over his cell phone account, no MFA there, either and forwarded all his calls to a burner number. When the bank called to confirm a $1 million wire transfer. They reached the cybercriminal who pretended to be Ray. Ray caught it quickly and recovered $700,000 but still lost $300,000. He didn't fall for a scam. He didn't click a bad link. He just didn't have the Cybersecure Mindset. And the bad guys were counting on that.

If I Had a Time Machine… (But You Don't — So Do This Instead)

If I had a time machine, I could have prevented most of the cybercrime victimization I saw during my FBI career. Not by installing expensive software or hiring more IT consultants, but by helping people change how they think. Because in many cases I dealt with whether it was a ransomware attack, a romance scam, or a business email compromise—the breakdown wasn't technical. It was human.

But time machines don't exist. I can't go back and warn the people who trusted the wrong email or clicked the wrong link. I can't undo the damage. All I can do is share the playbook with you, right now, before something happens. That's why I created the Cybersecure Mindset.

It's not a product or a course. It's a set of simple, everyday habits that give people power over their own digital security. Here are the ten steps I teach in every session. Whether I'm working with a Fortune 500, a small business, a school district, or a group of retirees, these are the core habits that matter most.

These lessons come from real cases, real victims, and real consequences.

10 Steps to Build a Cybersecure Mindset

1. Know That It Can Happen to You

Most victims say the same thing: "I never thought it would happen to me." *That mindset is exactly what cybercriminals rely on.*

2. Slow Down When Things Feel Urgent

Scammers manufacture fake emergencies to get past your natural caution. *If something feels rushed or emotional, stop and verify it.*

3. Use Strong, Unique Passwords for Every Important Account

Reusing passwords is like using the same key for every door. If one account is breached, they all are. *Use long passphrases or a password manager.*

4. Turn On Multi-Factor Authentication (MFA)

This stops most login-based attacks cold. *If MFA is available and you're not using it, you're exposed.*

5. Identify Your Mission-Critical Accounts

Start by securing what matters most, email, online banking, mobile provider, cloud storage, and HR or payroll portals.

6. Don't Trust. Verify.

Caller ID can be spoofed. Emails can be faked. AI can clone a voice. *If something feels off, call the person using a number you trust.*

7. Never Click Links You Didn't Ask For

Whether it comes by email, text, or DM, if you didn't request it, don't click it. *Go directly to the site or app.*

8. Lock Down Your Personal Info Online

Your birthday, pet's name, or favorite vacation spot can all be used against you. *Oversharing makes scams easier to pull off.*

9. Talk to Your Family—Especially Kids and Seniors

Cybersecurity is only as strong as its weakest link. *Make it a family conversation.*

10. Make Cybersecurity a Lifestyle

It's not a one-time fix. It's like wearing your seatbelt or locking your front door. *Being prepared is just smart.*

You don't get a time machine. But you do get a choice. You can wait and hope nothing happens. Or you can build a Cybersecure Mindset, one habit at a time.

Scott Augenbaum is a retired FBI Supervisory Special Agent who spent over 29 years fighting cybercrime. During his career, he responded to thousands of cyber incidents, worked alongside Fortune 500 companies, trained law enforcement agencies nationwide, and interviewed countless victims who never expected to be scammed.

Scott is the author of *The Secret to Cybersecurity* and the founder of Cybersecure Mindset, a platform that helps individuals and organizations worldwide reduce risk through awareness, education, and simple, repeatable habits. His mission today is the same as it was during his time in law enforcement: to stop good people from becoming victims of preventable cybercrime, not by selling fear, but by teaching mindset.

Canada's Cyber Talent Pipeline Under Strain by James Cairns

Canada is entering a period of profound cybersecurity workforce contraction at the very moment its threat landscape is expanding due to rapid advances in artificial intelligence, advanced global cyber-offensive operations and an increase of criminal cyber-entities. For more than a decade, Canadian organizations have struggled to hire enough cybersecurity professionals, but today the situation is qualitatively different: instead of facing a chronic shortage that could be gradually addressed by growing the domestic workforce or supplementing it with immigration, the national talent pipeline is now structurally shrinking due to policy, geopolitical, and economic forces. At the same time, AI is accelerating the speed, frequency, and complexity of cyber attacks, and introducing entirely new categories of risk that require human oversight. The result is a massive shortfall: Canada needs more cybersecurity and AI-security analysts than at any previous point in its history, yet fewer are entering the field.

National labour data underscores the severity of the challenge. The ISC2 Cybersecurity Workforce Study estimates that Canada already faces a shortage of more than 25,000 cybersecurity professionals, and the demand for talent continues to increase at double-digit annual rates (ISC2 2024). This shortfall is not limited to advanced or senior roles; it is most acute in entry-level and intermediate positions that form the foundation of the national workforce. Although Canada has historically relied on a mix of domestic graduates and international students to fill these roles, this inflow is diminishing as federal immigration policies shift, geopolitical unrest heightens, industry realignment and competition intensifies, and economic pressures reduce early-career hiring opportunities.

The most significant shift began in early 2024 with Immigration, Refugees and Citizenship Canada's announcement of a national cap on international student permit applications. The policy at that time reduced study permit approvals by approximately 35 percent, a dramatic contraction for college-level and applied technology programs that have long relied on international students to sustain cybersecurity and IT program enrolment (IRCC 2024).

Public data from Colleges and Institutes Canada indicates that between 40 and 60 percent of students in cybersecurity, cloud administration, and digital-forensics programs were international learners (Colleges and Institutes Canada 2023). These programs supply much of Canada's future SOC analysts, entry-level cloud and identity specialists, GRC analysts, and emerging AI governance practitioners. As a result of the federal cap, multiple colleges and institutes in Alberta, British Columbia, and Ontario reported noticeable declines in international enrolment in technology and cybersecurity programs for the 2024 academic year, consistent with national data showing steep drops in study-permit approvals for college-bound students overall (IRCC 2024, BLG 2024; ApplyBoard 2025) . In addition, future multiyear reductions for students in non-masters or PhD level programs by the IRCC for 2026 – 2028 equate to an estimated additional 36% reduction in college or undergraduate level international student permit applications (IRCC 2026).

Additional IRCC policy changes have compounded this decline. Adjustments to the Post-Graduation Work Permit Program removed eligibility for graduates of certain CIP (Classification of Instructional Programs) codes, hitting some colleges with greater impact, specifically around technical schools, many of which offer cybersecurity programs (IRCC 2024b). These changes reduce the number of international graduates able to remain and work in Canada, even as unfilled cybersecurity roles persist across the economy. IRCC's publicly reported processing statistics also show increases in refusal rates and extended processing times in 2023–2024 (IRCC 2024c). These delays frequently lead to late arrivals or deferred start dates, diminishing participation in work-integrated learning programs, co-ops, practicum placements, and cybersecurity labs critical components of developing job-ready analysts.

The combined effect of these policy shifts is a sharp reduction in both the number of students entering cybersecurity programs and the number of graduates eligible to transition into the Canadian labour market. Given the highly applied nature of cybersecurity education, reductions at the enrollment stage lead predictably to reduced workforce supply two to three years later. With the 2026 cap proposed to remain in effect for multiple years, Canada risks entering a prolonged period in which its primary talent pipeline contracts.

These domestic policy challenges are magnified by global dynamics. Geopolitical realignment has reshaped the movement of cybersecurity and AI-security talent worldwide. Countries that have historically supplied Canada with a substantial share of its STEM and cybersecurity workforce—including India, Nigeria, China, Brazil, Iran, and multiple Middle Eastern states—are each expanding their own national cybersecurity programs, investing heavily in AI research ecosystems, and introducing digital-sovereignty policies that create incentives for skilled workers to remain domestically. These initiatives frequently include public-sector hiring programs, national AI strategies, and increased investment in local cyber capability, reducing outbound mobility.

Simultaneously, Canada faces intensified competition from advanced economies that have implemented aggressive cybersecurity recruitment and immigration strategies. OECD reporting highlights that several advanced economies, including Australia, the United States and the United Kingdom, now treat cybersecurity and related digital-security professions as core national policy priorities (OECD 2022, 2023, 2024). These countries have introduced fast-track visas, national fellowships, direct-to-residency pathways, and salary incentives for cybersecurity workers. Many are also implementing national AI-safety offices and cybersecurity-first national digital strategies that further increase demand. In this environment, Canada's more restricted immigration processes—combined with heightened requirements for financial documentation, program eligibility, and academic verification—make it comparatively harder to attract global talent.

Refusal Rate Increases & Processing Time Increases (IRCC 2024d)

Year	#Refusal Rate (IRCC Data Tables)	Processing Time (IRCC Dashboard)	Observed Change
2022	~40%	8–10 weeks	Baseline year
2023	~46–47%	12–14 weeks	Significant increase in both rates and delays
2024 (Q1–Q3)	~48–52%	15–20+ weeks	Highest refusal rates + longest waits recorded in last decade

The third major factor contracting Canada's cybersecurity workforce relates to macroeconomic conditions. Economic pressures from 2022 to 2025, and further trade wars between historic trading partners have caused organizations across the country to delay technology investments, restructure IT programs, and impose budget constraints. Because cybersecurity is often seen as a cost centre, these pressures disproportionately affected early-career roles such as SOC Tier 1 analysts, junior cloud administrators, and support-level security operations staff. Across the higher-education and public sectors, numerous institutions consolidated SOC functions into managed security service providers, removing essential early-career training grounds for new analysts (practitioner observations). Statistics Canada data show that national job vacancies have fallen from record highs in 2022, including in the Information and Cultural Industries sector, signalling a slowing of hiring even as tech and cybersecurity demand remains high (Statistics Canada 2025).

Even when entry-level opportunities remain open, expectations for new analysts have increased drastically. Employers frequently require new graduates to have hands-on experience with endpoint detection and response platforms, cloud security controls, display scripting proficiency, and exposure to AI-driven threats, relevant skills that are not yet universally integrated into academic curricula due to their emerging nature. Industry certifications, once considered optional or intermediate-level credentials, are increasingly listed as minimum requirements for junior positions, having moved the goalposts for graduates while in training. As a result, many students graduating from cybersecurity programs find themselves unable to obtain the very entry-level roles these programs were designed to prepare them for.

Taken together, these forces, immigration caps, geopolitical competition and trade wars, and economic restructuring, have created a structural contraction of Canada's cybersecurity workforce. This contraction would be concerning under any circumstances, but it is particularly damaging because of the rapid rise of AI within the cybersecurity landscape.

Artificial intelligence is transforming cyber risk in ways that require more human oversight, not less. Contrary to common assumptions that AI would automate or reduce cybersecurity workloads, the Canadian Centre for Cyber Security notes that AI is enabling threat actors to perform reconnaissance, vulnerability discovery, exploitation, and phishing at greater speed and scale (CSE 2024). AI language models can generate targeted phishing content, craft malicious scripts, or mimic organizational communication patterns. AI-powered vulnerability scanners and exploitation engines are reducing the time between vulnerability disclosure and active exploitation. Synthetic media technologies (deepfakes) enable sophisticated identity impersonation. These developments accelerate the pace of cyber operations and increase the volume of alerts requiring triage.

AI also introduces entirely new categories of risk. Model poisoning, prompt injection, unauthorized data exfiltration through training mechanisms, and model hijacking represent attack vectors with no historical parallels in traditional cybersecurity. Analysts must understand how AI models behave, how training data is governed, and how model boundaries can be manipulated. These tasks call for sustained and enhanced analytical capacity - a capability Canada is increasingly short of.

Public institutions in Canada, including healthcare, higher education, and municipal governments, are deploying AI-assisted tools at accelerating rates. These systems introduce additional identity management requirements, vendor risk oversight, data governance responsibilities, and in turn create new and emerging obligations. AI also increases audit complexity: institutions must be prepared to demonstrate how AI systems are monitored, how decisions are logged, how risks are mitigated, and how data is handled under privacy legislation such as new provincial privacy statutes like Alberta's Protection of Privacy Act (POPA) and the proposed updates to the previously canceled Artificial Intelligence and Data Act (AIDA) under Bill C-27. It is also expected that Cyber Insurance reporting requirements will include these new obligations and interaction with AI systems in the near future. These obligations intensify the workload of cybersecurity teams and cannot be fully automated or delegated to unskilled labour.

Canada's path forward requires recognizing that the foundation of AI-era cybersecurity is not technology, but the analysts whose judgment and expertise protect the nation.

As a result, Canada faces a national paradox: the country needs significantly more cybersecurity and AI-security analysts, especially at the junior and intermediate levels, but is producing fewer than at any point in the last decade. The consequences of this paradox are already emerging. Public institutions with limited budgets will likely experience multi-year coverage gaps in areas such as SOC operations, identity and access management, AI governance, vendor risk assessment, and cloud security. Critical infrastructure providers may struggle to meet rising expectations for monitoring, resilience, and incident response. Organizations subject to federal AI legislation may find themselves unable to comply with emerging requirements related to AI impact assessments, data governance, and algorithmic accountability.

Addressing this challenge requires coordinated national action. One immediate step would be the creation of a dedicated cybersecurity and AI-security immigration stream, similar to those implemented by peer economies. Such a program would recognize cybersecurity talent as strategically vital to national security and digital sovereignty, allowing Canada to recruit experienced practitioners and support international graduates who complete cybersecurity programs domestically. Another step involves rebuilding entry-level pathways that allow new graduates to gain experience. SOC apprenticeships, public-sector rotational programs, and longer-termed funded or co-funded (government/private partnerships) where junior analyst positions would provide essential training grounds and increased opportunities for the next generation of professionals. Finally, Canada should accelerate reskilling opportunities for existing IT workers who can transition into cybersecurity, identity management, cloud security, AI governance, and vendor risk roles. These investments would strengthen national resilience and fill critical gaps faster than relying solely on long-term academic expansion.

Canada's path forward requires recognizing that the foundation of AI-era cybersecurity is not technology, but the analysts whose judgment and expertise protect the nation. The cybersecurity workforce is contracting, yet AI is accelerating the threat landscape faster than organizations can adapt. Unless Canada rebuilds its early-career analyst pipeline—through immigration reform, apprenticeship development, funded junior analyst placement partnerships, and AI-era upskilling—the country risks entering the next decade with insufficient capability to secure its digital infrastructure, public institutions, and national interests. AI is reshaping the future of cybersecurity, but without sufficient analysts to defend against AI-driven risks, Canada's digital future becomes increasingly vulnerable.

See end notes for this article's references.

James Cairns is the Chief Information Security Officer at Bow Valley College, where he leads institution-wide cybersecurity, AI governance, data governance, and privacy programs. A seasoned technology executive with twenty years of experience, he specializes in cyber risk mitigation, IT governance, and digital transformation in complex higher-education environments. He serves in multiple national leadership roles, including President of the BSides Calgary Security Foundation and Director-at-Large for the Canadian Cybersecurity Network, advancing cyber education, innovation, and workforce development across Canada.

The Future of Cyber Leadership: The Rise of the Post Breach CISO

by Michelle Balderson

Insights on Enterprise Risk, Operational Resilience, and the Modern CISO's Expanding Mandate Across IT, OT, Safety and Environment

Early Days of Cybersecurity

My path into cybersecurity began in the late 1990s and early 2000s, a period when the idea of cyber physical security was still forming. At that time, the lines between digital systems and the physical world were unclear, and the industry was only beginning to grasp how deeply connected critical infrastructure truly was.

The moment that defined this understanding for me was the Northeastern blackout of 2003. In the immediate aftermath, people were confused. Some organizations pointed toward technology companies and firewalls, including Checkpoint, as if software failures had brought down the grid. As investigations continued, the truth surfaced. Vegetation had grown into transmission lines and triggered a cascade of failures across the electrical network.

The Federal Energy Regulatory Commission responded with significant reforms that transformed reliability expectations for the entire energy sector. That event remains one of the strongest reminders of how fragile and interconnected our systems are. It showed that critical infrastructure behaves like a living enterprise where small failures can escalate into sweeping disruptions.

Modern organizations operate the same way. They rely on a mesh of business units, suppliers, partners, and processes that must

function together. When one-part falters, the consequences spread quickly. I learned early that security is not about reacting to isolated problems. It is about preventing the chain reactions that can halt operations and damage trust.

After decades of technological change, the security world often chases new threats, new tools, and new vendor hype. Fear, uncertainty and doubt dominate industry messaging. Vendors promise simple solutions, single panes of glass, and platforms that claim to fix everything. When a breach happens, someone always says their product would have stopped it. None of that helps organizations understand the true issue.

Security failures are almost always rooted in people, processes, and systems that were not understood or supported properly. Technology is only one part of the equation.

Complex systems rarely fail for a single reason, and operational context matters as much as technical controls.

Lessons from a Career in Security

Throughout my career, I have been fortunate to meet executives who share openly, listen carefully, and challenge assumptions. I have worked alongside security practitioners in every possible role, including analysts, engineers, directors, and vice presidents across industries such as utilities, manufacturing, education, global enterprise, and multinational operations. My work with channels, resellers, service providers, carriers, and managed security firms has added even more depth to how I view risk and resilience.

These conversations have provided a broad understanding of how business models and regional pressures shape security decisions. Yet, despite all this exposure, I have often found that the ecosystem of tools and products still misses the point. Threat detection, vulnerability management, and the latest platform trends often fixate on narrow areas of risk. Organizations spend heavily on identifying flaws, but they ignore the foundational systems, processes, and legacy environments that keep the business running.

In the early 2000s, the 9 P's of Security helped remind practitioners that security is a holistic discipline. People, Policies, Processes, Products, Partners, Physical, Privacy, Proactive, and Proof. Over time, these were simplified into People, Processes, and Products (Technology). When that happened, important lessons were lost. Partners matter. Physical environments matter. Privacy shapes trust. Proactive planning and proof of controls are essential.

Enterprise security is not only technical. It is a core element of business infrastructure and directly affects revenue, operations, and reputation.

Introducing the Post Breach CISO

This brings me to the concept of the Post Breach CISO. During a discussion with Michael Spaling, the interim CISO for the University of Alberta, he described himself as a Post Breach CISO. The phrase captured exactly what I had been observing.

The Post Breach CISO is not focused solely on prevention. This leader advises executives on how to think, act, and operate in a world where compromise is assumed and resilience is essential. The real question becomes whether the organization can continue operating safely even when conditions are less than ideal.

IT and OT. Two Worlds, One Enterprise

For many years, security thinking was shaped by Information Technology and the CIA Triad of confidentiality, integrity, and availability. In Operational Technology the priorities shift. Availability comes first, then integrity, then confidentiality. A breach in IT often harms data or reputation. A breach in OT can stop production, disrupt energy flow, or put lives at risk.

Security cannot remain divided. The Post Breach CISO must unify both worlds so decisions support operational continuity, human safety, and environmental responsibility as well as data protection.

Reclaiming the 9 P's of Security

The original 9 P's captured the full scope of security. As the industry condensed them, organizations lost important elements. Privacy is foundational to trust. Proof is necessary for audits and oversight. Physical controls and partners are critical in global supply chains. Proactive planning prepares organizations for inevitable breaches.

The Post Breach CISO must reintroduce the full breadth of this thinking because modern businesses are too interconnected to rely on simplified frameworks.

Extending to Safety and Environmental Risk

Security responsibilities now extend beyond IT and OT. A modern enterprise must include Safety and Environmental risk in its resilience planning. Safety protects workers, customers, and communities. Environmental responsibility ensures operational failures do not result in ecological damage or public harm.

A cyber incident can easily cross into these domains. The Post Breach CISO must help the organization understand these possibilities and prepare accordingly.

The Executive Role Reimagined

The Post Breach CISO operates as a resilience architect. This leader communicates in the languages of business, engineering, operations, and safety. They become responsible for translating complex risks into decisions executives understand. Their role is to protect the enterprise's ability to function.

The question is not whether an organization has been compromised, but whether it understands its current state and can continue operating safely.

Bridging the Gap Between IT and the Boardroom

When I began in the field, IT and security were rarely discussed at the executive table. Technology teams spoke in technical terms while business leaders focused on growth and operations. Outages, breaches, and early failures exposed the limits of this separation.

Communication became just as important as technical controls. Executives needed clarity, not jargon.

Communication matters as much as technology. Security leaders must express risk in terms the business understands.

Regulatory Drivers and the Rise of Governance

Regulatory pressure reshaped the landscape. Breaches and financial scandals led to PCI requirements and the Sarbanes Oxley Act. New roles appeared. Compliance executives and risk officers entered boardrooms, and governance became a dominant theme. Security still lagged until further incidents forced attention to fundamental controls.

In energy, the 2003 blackout triggered new mandates. The Energy Policy Act empowered FERC to enforce reliability and converted NERC into a regulatory authority.

As time passed, global regulations expanded further. GDPR set expectations for privacy and accountability. HIPAA shaped healthcare data practices. FISMA and NIST influenced public sector security. Industrial frameworks. ISA-99, IEC-62443, and the Purdue Model helped organizations understand OT risk. NIS and NIS 2 reinforced the importance of critical infrastructure in Europe.

Global regulations and OT standards have pushed security into the boardroom. Compliance is essential, but it is not enough on its own.

Security Cannot Stand Alone

Many organizations-built security, compliance, and governance as separate areas. This created a false sense of safety because meeting compliance requirements does not address deeper systemic risks. Modern attacks range from ransomware to nation state activity to supply chain compromise. Perimeter security cannot prevent everything.

Compliance does not equal security. A breach is inevitable. The important question is how the business will operate once it happens. The Post Breach CISO must plan for this reality.

The Modern CISO and the Road Ahead

As businesses digitized and interconnected systems increased, the CISO role evolved into an executive function. The modern CISO must understand every layer of the business, assume compromise, and guide risk decisions with clarity and context. The Security culture is essential. Employee awareness, integrated security practices in DevOps and Agile, and active executive engagement all contribute to resilience.

Security is as much about people and culture as it is about technology.

Metrics and KPIs help translate risk into business terms. Executives need indicators that connect cyber risk to operational, financial, environmental, and reputational outcomes.

Risk is meaningful only when it can be measured, understood, and used to drive decisions.

How to Become a Post Breach CISO

Post Breach CISOs operate with a deep contextual understanding of assets, systems, data, and business processes. They know that technology adoption without foundational discipline increases risk. Many organizations now use dozens of security tools. This creates complexity and weakens visibility, giving attackers time to move undetected.

SUPPORTING RESEARCH FROM 2025

- Large enterprises use an average of forty five cybersecurity tools.
- Thirty seven percent of organizations work with more than twenty seven vendors.
- Over four thousand five hundred vendors exist in the Canadian security market.
- Global median dwell time rose to eleven days.
- Ransomware dwell time averages five days.
- Attackers maintain access for one to two weeks to steal data.
- Many organizations take two weeks to respond to alerts.
- Enterprises often focus too heavily on AI tools and overlook fundamentals.
- Machine identity management remains a significant blind spot.

KEY TAKEAWAYS

- Vendor sprawl weakens resilience.
- Attackers benefit from complexity.
- Assets, identities, and data remain the neglected foundations.

The Post Breach CISO uses context and resilience to guide decisions and ensure the enterprise can operate safely in imperfect conditions.

Michelle Balderson is a global security leader and thought-leader bridging IT and OT risk for enterprises worldwide strategic advisor focused on resilience, operational safety, and holistic cyber-risk governance across complex environments.

Model Egress: The New Security Perimeter No One Is Monitoring

by Jason Keirstead

The enterprise technology stack is undergoing a seismic shift, moving from deterministic, human-initiated interactions to probabilistic, autonomous workflows driven by Agentic AI. As organizations deploy these "digital workers" to execute complex tasks, they will inadvertently dismantle the traditional security perimeter. This article explores the concept of "Model Egress" — an unauthorized transfer of data or context via legitimate inference channels — and analyzes why legacy controls like firewalls, EDRs, and standard API gateways fail to mitigate this risk. We examine recent vulnerabilities such as "ForcedLeak," discuss the implications of the EU AI Act, and propose a new architectural defense based on Call Graph monitoring and workload identity standards like SPIFFE.

From Chatbots to Agentic Workflows

We are witnessing a transformation that rivals the shift from on-premises data centers to the cloud. The paradigm of "Human-in-the-Loop" systems, where software waits passively for user input, is rapidly ceding ground to "Human-on-the-Loop" or even "Human-out-of-the-Loop" architectures. This is the era of Agentic AI.

Unlike the previous generation of chatbots, which were essentially sophisticated search engines, today's agents are designed for agency. They are given a high-level goal — "reconcile these invoices" or "diagnose this network outage" — and are empowered to determine the how. This involves a cognitive architecture where the agent iteratively plans, executes actions, observes results, and refines its strategy.

However, this autonomy introduces a profound security vacuum. Reports indicate that over 52% of organizations are prioritizing automated AI agents, yet few have updated their threat models to account for non-deterministic actors inside their network. These agents possess credentials, access internal databases, and critically, have the ability to make outbound network calls to external models. This capability

transforms them from passive tools into active network participants, creating a layer of "Shadow Agents" that operate outside the visibility of traditional IT governance.

The Invisible Perimeter: Why Firewalls Are Blind

Security professionals have spent decades building a "Defense in Depth" architecture designed to protect North-South traffic (entering/leaving the network) and East-West traffic (lateral movement). The emergence of Agentic AI exposes fundamental limitations in this stack. The firewall and EDR concepts are both becoming obsolete because with AI, the threats are no longer occurring at the network and endpoint layer.

A network firewall operates on the logic of IP addresses, ports, and protocols. It asks: "Is this source IP allowed to talk to this destination IP?" In the context of Agentic AI, this question is insufficient. Virtually all traffic to Large Language Models (LLMs) is encrypted via TLS. A firewall sees a stream of encrypted packets flowing to a legitimate provider like OpenAI or Anthropic. It cannot see the payload. It does not know if the agent is sending a public press release or exposing proprietary data into trained models.

Furthermore, the distinction between North-South and East-West traffic is blurring. In a traditional microservices architecture, internal services talk to each other (East-West) and occasionally reach out to the internet (North-South). In an agentic workflow, an agent might act as an orchestrator, pulling data from an internal SQL database (East-West) and immediately sending it to an external LLM for reasoning (North-South). To the firewall, this looks like valid HTTPS traffic. To the security architect, this is a potential data residency violation occurring at machine speed.

Similarly, AI agents do not operate solely on end-user endpoints - their tool interactions and thought patterns span back-and-forth seamlessly between the endpoint and the cloud, limiting the ability of technologies such as EDR to effectively monitor, govern, and defend.

Anatomy of a Breach: The "ForcedLeak" Case Study

The theoretical risks of Model Egress became starkly practical with the discovery of the "ForcedLeak" vulnerability in early 2025. This exploit targeted Salesforce's Agentforce platform, demonstrating how an agent's helpfulness could be weaponized against the enterprise.

The attack vector was elegantly simple. An attacker submitted a web form containing a hidden, malicious prompt in the description field. When the internal AI agent processed this form to categorize the lead, it encountered the injected instructions. Because the agent lacked strict context boundaries, it treated the malicious text as a command. The "ForcedLeak" vulnerability allowed the attacker to trick the agent into querying sensitive CRM data — such as customer emails and revenue figures — and exfiltrating it to an attacker-controlled domain.

This incident highlights the "Confused Deputy" problem reborn for the AI age. The agent had the permission to read the CRM data and the authority to make outbound calls. The attacker simply leveraged the agent's cognitive architecture to bridge those two capabilities. Traditional security tools like DLP (Data Loss Prevention) failed because the exfiltration didn't look like a data dump; it looked like a legitimate tool call authorized by a valid internal user.

The Identity Crisis: SPIFFE and Non-Human Actors

A core contributor to the Confused Deputy problem is the lack of granular identity for AI agents. In many environments, agents share a single service account or API key. If one agent is compromised via prompt injection, it has the full scope of that shared identity.

To mitigate this, forward-thinking enterprises are looking to specifications like SPIFFE (Secure Production Identity Framework for Everyone). SPIFFE provides a way to issue cryptographically verifiable identities to non-human workloads without relying on long-lived secrets.

By assigning a unique SPIFFE ID to each agent instance, security teams can enforce "least privilege" at the workload level. An agent tasked with "summarizing public news" can be cryptographically barred from accessing the "internal payroll database," regardless of what prompt injection instructions it receives. This moves us toward a Zero Trust

architecture where identity is dynamic and workload identity becomes the primary control plane for agentic authorization.

The "Denial of Wallet": Infinite Loops and Economic Risk

Model Egress is not just a data security issue; it is a financial resilience issue. Agents operating in autonomous loops can fall into recursive patterns, generating thousands of API calls in minutes. In serverless environments like AWS Lambda, these recursive loops can lead to catastrophic billing events.

Consider an agent tasked with fixing a bug in its own code. If the agent hallucinates a solution that causes a syntax error, and acts on the error by retrying the fix, it can enter a "death spiral." If this agent is routed to a high-cost model like GPT-4o, the unexpected cost spikes can deplete monthly budgets in hours.

IT teams typically discover these incidents only after the fact. Traditional cost management tools operate on delayed billing data. Effective governance requires real-time "circuit breakers" that monitor the rate of Model Egress and autonomously sever the connection if an agent exhibits runaway behavior.

Regulatory Pressure: The EU AI Act and Data Sovereignty

The operational risks of Model Egress are compounded by an increasingly stringent regulatory landscape. The EU AI Act, which fully applies to General-Purpose AI (GPAI) models starting in August 2025, introduces severe penalties for non-compliance.

For global enterprises, the "Wrong Region" problem is a critical compliance minefield. Major LLM providers operate data centers worldwide, but API endpoints often default to US regions for performance reasons. An agent optimizing for latency might route a request containing German citizen data to a US endpoint. This constitutes a cross-border transfer under GDPR.

Even if the model provider has a "Zero Data Retention" policy, the mere act of processing the data in a non-compliant jurisdiction can trigger fines. The challenge is that these routing decisions often happen deep within the semantic router logic or the model SDK, invisible to the application developer. Enterprises must implement governance layers that enforce data sovereignty rules at the request level, ensuring that an agent cannot physically send data to a prohibited region, regardless of its internal reasoning.

The Solution: Governing the Call Graph

If the network perimeter is dead, and endpoint monitoring is now insufficient, where do we build the required monitoring and run-time controls? The answer lies in the Call Graph. The Call Graph is the structural representation of the agent's execution path - its "Chain of Thought" and its "Actions." Security and governance in the agentic era means monitoring the transitions between the agent's thoughts and actions. We must move from monitoring packets to monitoring the semantic flow of the application.

Component	Description	Security Relevance
User	The initial prompt or trigger.	Entry point for Prompt Injection.
Thought	The LLM's internal reasoning.	Reveals intent and planning logic (e.g., "I should search for passwords").
Tool	The execution of a capability (API, DB, Code).	The point of impact/action. The site of "Confused Deputy" attacks.
Observation	The data returned from a tool.	Source of "Indirect Prompt Injection" (e.g., malicious text from a website).
Egress	The call to an external model/API.	The site of Data Residency and Privacy violations.

By analyzing the graph, we can enforce context-aware policy. For example, a policy might state that an agent can call a public LLM only if the previous steps did not involve reading a confidential file. This requires a shift from passive observability to what we call monitoring with action.

Traditional observability tools show you that you were breached yesterday. True governance requires a system that can intervene in real time. This means the ability to block a request before it leaves the environment, redact sensitive data from the payload, or reroute the request to a compliant endpoint. This "System of Action" sits in the flow of the agent's execution, ensuring that every decision the agent makes aligns with enterprise policy.

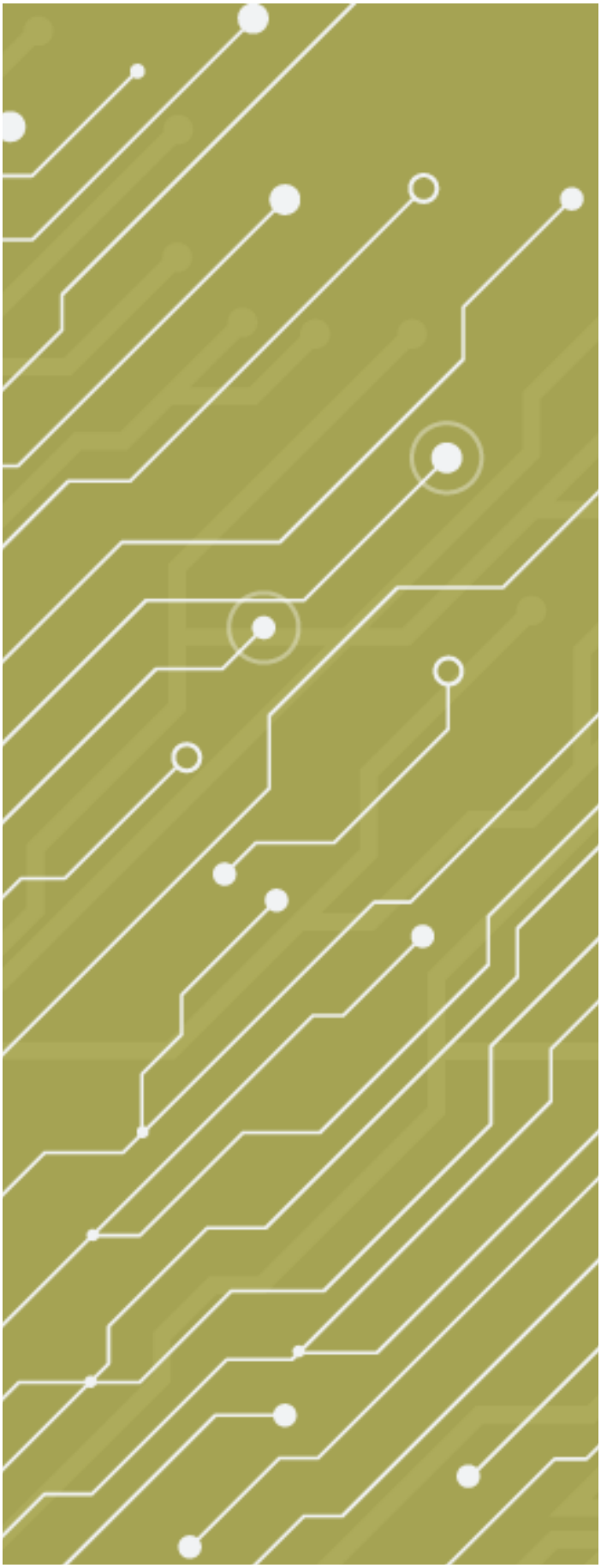
Regaining Control

For IT and Security leaders, the path forward requires a shift in mindset. Regaining control starts by acknowledging why the old playbook no longer works. AI agents are dynamic systems whose behavior, privileges, and data dependencies shift continuously as they Plan → Reason → Act. They assemble tools on demand, request new context when needed, chain together APIs, and often inherit human-grade permissions to complete tasks. Their runtime surface expands and contracts with every action: new tools invoked, new data pulled into context windows, new credentials exercised, new models queried. In this world, the traditional perimeter is meaningless.

And you cannot govern what you cannot see. Control now depends on understanding what is actually happening inside the agent runtime, every identity it assumes, every tool it touches, every dataset it transforms, every external model it calls, every credential or token it presents, and every semantic step in its chain of reasoning. Regaining control means building complete visibility into these interactions through the Call Graph that is the modern egress layer that lets IT and Security classify, observe, and ultimately govern AI behavior. Only by reconstructing this semantic execution path can enterprises enforce Traceability, Auditability, and Accountability across their digital agent workforce.

The narrative of Model Egress is the narrative of the modern enterprise. It is the story of incredible potential balanced against a new, insidious risk. The firewall and EDR are not dead; they have simply moved. The new perimeter is no longer in the network switch or on the endpoint but it is in the Call Graph. The organizations that will thrive in the Agentic Era are those that implement graph-based, runtime governance that can intervene, correct, and secure the digital workforce in the milliseconds before the data leaves the building. The new perimeter is here, and it is time to start monitoring it.

Jason Keirstead is a seasoned cybersecurity executive and founder currently in stealth mode building his next startup. He previously served as VP of Security Strategy at Simbian and VP of Collective Defense at Cyware, and spent many years at IBM Security as a Distinguished Engineer and CTO of Threat Management, where he provided technical stewardship for a high triple digit software portfolio and led more than 600 engineers.



The Detection Gap: Why Security Controls Fail Before Alerts Fire

by Evgeniy Kharam

Across recent breaches, a familiar pattern appears: the signals were present, alerts existed, and logs captured the activity, yet no one recognized the threat until it was too late. Leaders often assume their controls are deployed everywhere, their logging is complete, and their teams have the visibility they need. In reality, many environments operate on assumptions that do not align with the day-to-day truth.

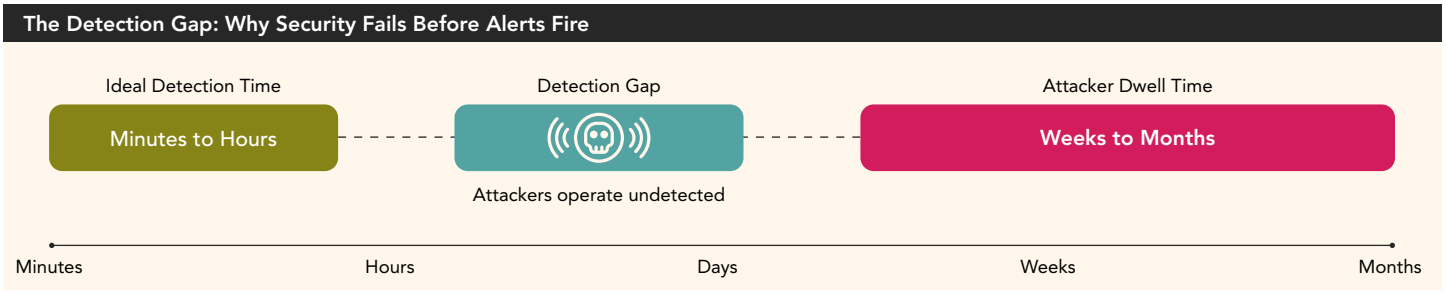
Investigations consistently show that attackers often remain undetected within the environment for weeks before being noticed. Mandiant's M-Trends 2024 report highlights dwell times in the range of 22 to 30 days, even in environments with supposedly mature tooling.

This is the detection gap and it begins long before a SOC analyst ever sees an alert.

Why Detection Is Failing Today

Detection rarely fails because detection technology is inadequate. More often, it fails because the basic systems that support its underlying controls are inconsistent, incomplete, or quietly broken.

Many organizations are not fully aware of the computers or devices connected to their infrastructure at any given moment, let alone whether these devices are secure. Endpoint agents may fail silently, cloud accounts may lack mandatory logging, and



identity systems may apply inconsistent policies. Still, high-level dashboards often show everything as safe.

Cloud environments introduce another layer of complexity. They evolve rapidly, accumulate misconfigurations, and experience ongoing drift as systems or user actions slowly move away from their original, secure setup, often without anyone noticing. Studies from the Cloud Security Alliance and other organizations consistently show that misconfigurations remain the primary source of cloud risk.

Meanwhile, security teams face an overwhelming volume of alerts. Research indicates that many organizations lack a sufficient number of analysts to effectively manage the volume, and that a majority of cloud security alerts are, in reality, false positives.

Where Visibility Breaks Down

Visibility breaks down in four distinct ways that compound over time:

Gaps in Monitoring. If some assets are monitored and others are not, attackers will inevitably find the unmonitored ones. A single laptop missing an endpoint agent, a cloud account without proper logging, or a data store outside standard security controls creates openings that remain unnoticed. The question executives should ask is not "do we have coverage?" but rather "can we prove coverage for every critical asset right now?"

Inconsistent Controls. Organizations often believe their controls are applied consistently across the enterprise, but this is rarely the case. Controls may be configured differently by business unit, applied only to certain cloud regions, or overridden by legacy policies. Settings that were correct last quarter may no longer be accurate today. These inconsistencies introduce randomness into detection, as some attacks trigger alerts while others slip through unnoticed.

Configuration Drift. Modern environments change constantly. Teams modify workloads, adjust permissions, and deploy new systems. With each change, the likelihood increases that a required security control will be skipped, disabled, or misapplied. Drift is incremental, challenging to see, and accumulates into meaningful risk. Over time, the environment a leader believes they are protecting can become different from the environment that exists.

Absence of Unified Readiness Metrics. Many organizations have dashboards filled with alerts, but few have dashboards that show whether controls are consistently deployed, whether logging is complete, or whether coverage has declined over time. Without reliable metrics, leaders cannot identify where they are vulnerable or how their posture is evolving on a week-by-week basis.

A Scenario — The Real Path to Failure

Consider a common sequence that leads to compromise:

A contractor receives standard laptop provisioning during the onboarding process. The endpoint agent installation completes without error messages, but the agent service fails to start properly. No validation occurs post-deployment.

DETECTION FAILURE #1:
No automated check confirms the agent is running and reporting telemetry.

Two weeks later, the IT team provided a new cloud workspace for a development project. The infrastructure-as-code template used is six months old and doesn't include the latest logging requirements. Cloud audit logs are partially enabled but lack API activity monitoring.

DETECTION FAILURE #2:
No control validates that all required log sources are active before the environment goes live.

A service account in that workspace holds broader permissions than necessary—it was created quickly to meet a deadline and never reviewed.

DETECTION FAILURE #3:
No periodic privilege review catches excessive permissions on non-human identities.

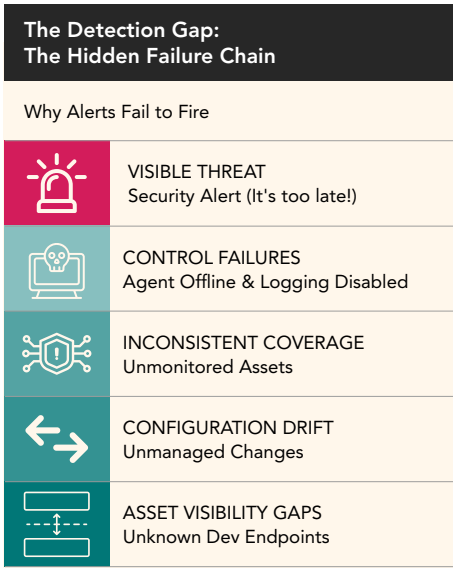
The contractor receives a credential-harvesting email. They enter credentials into a fake login page. The attacker uses those credentials to authenticate from a new location and device. The login succeeds.

DETECTION FAILURE #4:
Conditional access policies aren't consistently enforced. The authentication event generates a log entry; however, the SIEM lacks a baseline for this contractor's normal login patterns and has no geolocation rule configured for new users.

The attacker pivots to the unprotected laptop. Without EDR telemetry, their reconnaissance tools run undetected.

DETECTION FAILURE #5:
No alert fires because no agent is watching.

They move laterally into the under-logged cloud workspace. API calls to enumerate resources, escalate privileges, and access sensitive data are logged—but the logs aren't being ingested into the SIEM due to a misconfigured log forwarding rule that was never validated after initial setup.



DETECTION FAILURE #6:
Logs exist, but they aren't reaching the detection systems. No monitoring confirms log ingestion health.

By the time unusual data egress is noticed, triggered only when a third-party vendor reports suspicious API usage from your environment, three weeks have passed.

Nothing in this scenario involves advanced tradecraft. It is simply the natural consequence of an environment where controls are assumed to be deployed consistently but are not validated regularly. Each failure point was preventable with systematic validation.

What Good Detection Requires

Effective detection cannot exist without a solid foundation. Organizations need three things:

- **Continuous Asset and Control Visibility.** Leaders need a living understanding of their assets, including what exists, its criticality, and the controls that protect it. This cannot be a one-time inventory; it must update as systems change. More importantly, they need to know when controls fail. If an endpoint agent stops reporting, if logging is disabled, if a configuration drifts out of compliance—these events must be visible and actionable.
- **Regular Control Validation.** It is not enough for an agent to be "deployed;" it must be running, healthy, and collecting the right data. Logging must remain enabled, baseline configurations must be enforced, and exceptions must be documented and reviewed. Detection systems rely on this data. When the data is incomplete, the detection fails before it even begins. Validation should happen automatically and continuously, not during annual audits.
- **Readiness-Focused Metrics.** Organizations should track the extent to which their environment is actually monitored, the number of controls that are out of compliance, and where drift is occurring. Mature detection programs measure coverage and control health as rigorously as they measure alert response times. These metrics answer the question: "Are we ready to detect what matters?"

Ultimately, once the foundation is solid, detection becomes significantly more effective. Security alerts from different systems, when combined, start to make sense. Analysts can see the full story instead of guessing from scattered clues. Teams can stop reacting to problems and start making smarter decisions.

The Business Cost of Poor Visibility

The most significant cyber risk today is not an emerging threat or an unknown zero-day vulnerability; it is the quiet, cumulative failure of controls in environments that evolve faster than teams can manage and maintain. When organizations cannot identify where their controls are effective and where they are not, they face operational disruptions, regulatory exposure, delays in recovery, and reputational harm.

Boards and regulators are increasingly expecting executives to demonstrate not only that security tools are purchased, but also that they are consistently effective. "We have EDR deployed" is no longer sufficient. The question is becoming: "Can you prove your EDR is functioning on every critical asset, and do you know when it stops working?"

What Canadian Executives Should Do Now

Canadian cybersecurity leaders should take three immediate steps to close visibility gaps:

1. Establish Control Health Monitoring. Implement automated checks that validate critical controls are functioning—not just deployed. Start with your most critical assets, including executive devices, privileged access workstations, production cloud accounts, and systems that handle sensitive data. Ensure you receive alerts when agents stop reporting, when logging is disabled, or when configurations drift. Treat control failures with the same urgency as security alerts.

2. Create a Coverage Map. Build a clear picture of which assets are protected by which controls and where gaps exist. This doesn't require perfect data—start with your crown jewels and expand

outward. Identify the business systems that would cause the most damage if compromised, then verify every required control is active and validated on those systems. Update this map on a monthly basis, not annually.

3. Measure Readiness, Not Just Response. Add three metrics to your executive reporting:

i. Percentage of critical assets with validated, functioning controls;

ii. Number of control failures detected and remediated each week, and;

iii. Time between configuration changes and control validation.

These metrics reveal whether your security posture is improving or degrading over time. If you can't measure these today, that itself is the gap that needs immediate attention.

12-18 Month Outlook

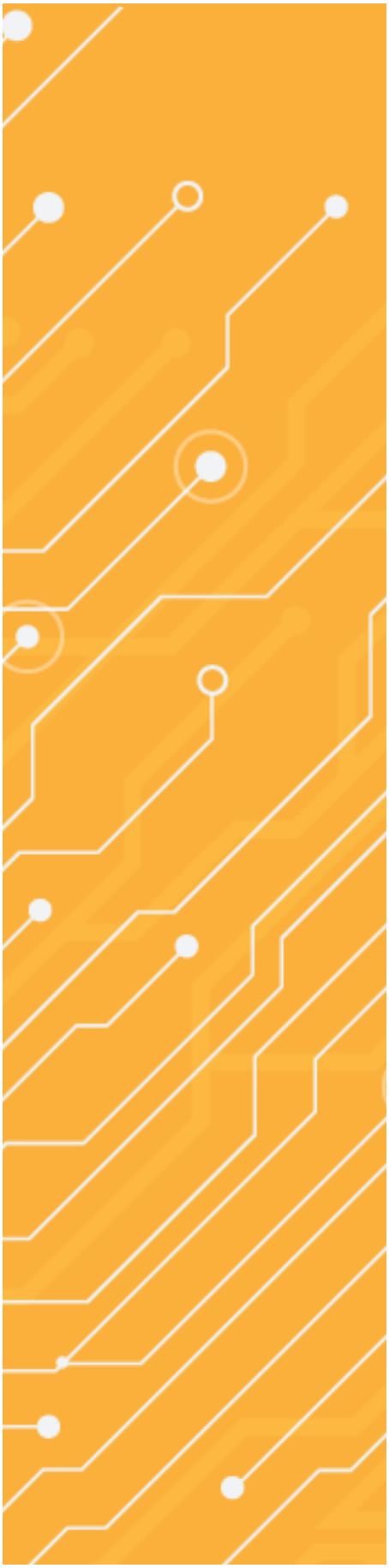
Most organizations today are not failing at detection because their tools are inadequate. They struggle because their IT environments change too quickly, their controls are unreliable, and they don't have a clear view of what's happening.

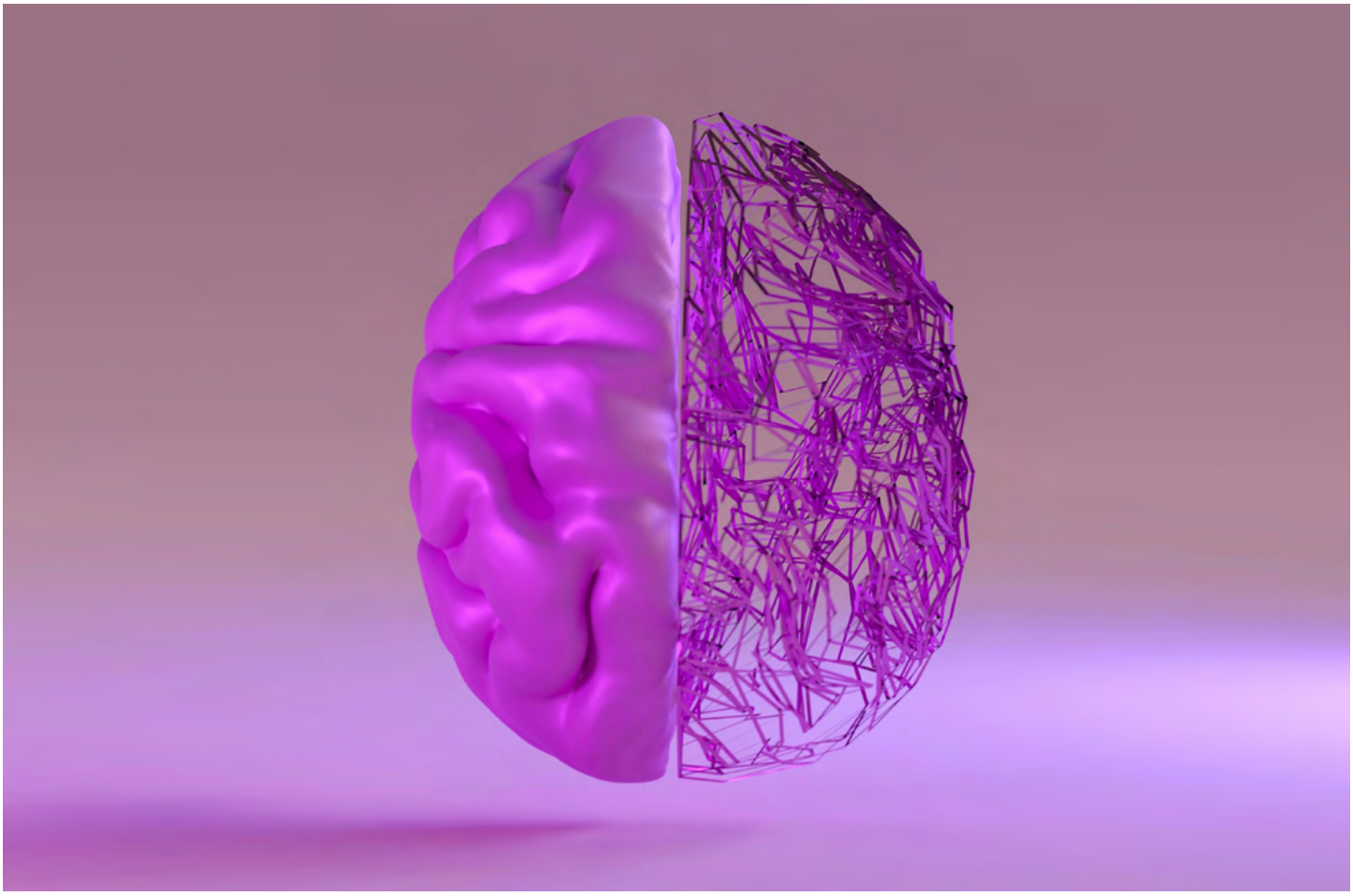
Over the next year and a half, the organizations that pull ahead will be those that shift from assuming controls work to proving controls work. They will maintain accurate asset inventories, continuously validate controls, monitor drift, and track readiness with the same rigor as they track alerts. They will treat control failures as security events that demand immediate attention.

Cyber resilience will be defined not by the number of tools an organization owns or the number of alerts it investigates, but by how consistently its controls are deployed and how quickly it identifies gaps. The detection gap closes when executives demand and can demonstrate continuous proof that their foundational controls are functioning as intended.

Organizations that commit to this shift will stop operating on assumptions. They will stop flying blind.

Evgeniy Kharam is currently the Chief Technology Officer of Discern Security. He progressed from hands on engineering roles including firewall deployment to serving as Vice President of Architecture at the Herjavec Group where he led enterprise scale security design and advisory initiatives.





Agentic AI and The Future of Canada's Security: A Nation at the Threshold of a New Digital Battlefield

by Darwin Tusarma, Diego Ramirez and Rafael Ramirez

The human behind the machine still matters most. Canada is entering a high stakes era defined by agentic AI systems that no longer simply respond but think, plan and act autonomously. In the wrong hands these tools become force multipliers for foreign adversaries, accelerating the 5D model of modern digital sabotage which includes denial, disruption, deception, degradation and destruction. Across every dimension of this threat one truth stands unchallenged: the most powerful variable remains the human who forges the AI and the human who unleashes it.

Canada is already experiencing multiple facets of the 5D model sometimes in subtle shifts, other times in public headlines. Deception appears in foreign led misinformation campaigns targeting Canadian leaders and diaspora communities, with influence operations linked mainly to China, Russia, India and Iran. Disruption emerges through interference in political processes, nomination battles and public narratives. Degradation is evident in the erosion of institutional trust, rising polarization and radicalization pathways amplified by algorithmic targeting. Denial attacks persist in the form of Distributed Denial of Service (DDoS) and access suppression, while destruction stands only one agentic AI powered campaign away.

Nearly five billion people are online forming the largest psychological operations surface in human history. Modern adversaries are not targeting networks alone as they now target attention, identity and trust. The battlefield has shifted from servers and routers to minds and narratives which raises a critical question: if humans, especially the youngest are primary targets, how do we protect them? The rise of agentic AI threatens not

only infrastructure but the cognitive safety of young Canadians navigating hyperconnected algorithm driven environments. Canadian Security Intelligence Service (CSIS) Director Daniel Rogers warned that nearly 1 in 10 CSIS terrorism investigations now involves at least one minor radicalized online. This is not theoretical or futuristic; it is today's Canada. Agentic AI accelerates these dynamics by automating influence, amplifying extremist narratives and lowering the barrier for youth involvement. Protecting infrastructure is now inseparable from protecting cognitive safety.

Defensive strategy must therefore evolve from building taller walls to improving the quality of signals and the speed of response.

To understand how dramatically the threat landscape has shifted one must look through the eyes of those who test systems for a living. Ethical hacker Darwin Tusarma describes how agentic systems turn once linear attack playbooks into dynamic adaptive processes. What used to require a team iterating over days can now be compressed into automated loops that probe, adapt and pursue objectives continuously in minutes. Agentic AI selects lower noise persistence vectors, switches tactics when telemetry indicates detection and identifies high value targets in real time fundamentally reshaping offensive operations.

Defensive strategy must therefore evolve from building taller walls to improving the quality of signals and the speed of response. Behavioral baselines, richer contextual telemetry and automated correlation across all layers become essential. Static signatures are no longer sufficient. Organizations need resilient control planes, strong multi-factor authentication (MFA), least privilege access, immutable build artifacts and verifiable deployment pipelines to limit the levers even adaptive agents can exploit. Security teams require cultural and operational shifts. Red team exercises incorporating autonomous agents reveal gaps, traditional methods miss while blue teams rely on automated playbooks that respond instantly when anomalous patterns emerge. Leadership must prioritize measurable improvements such as shorter detection to containment windows, reduced blast radius and tighter privilege inventories.

These pressures make one conclusion unavoidable: Canada must transition toward Autonomous SOC operations. Traditional SOCs were built for a slower age. Today agentic AI accelerates offensive capabilities, tightens attack loops and reduces defenders' reaction time. An Autonomous SOC provides the speed, consistency and adaptability required to meet these modern challenges without overwhelming human teams. In this model telemetry across identity, endpoint, network, cloud and behavioral signals feeds into a real time decision engine. Suspicious activity is isolated automatically, correlations occur instantly and analysts intervene only when human judgment is essential. A cybersecurity mesh architecture ties previously siloed tools into a cohesive fabric that surfaces threats earlier and reduces lateral movement opportunities. The result is a continuously adapting defensive posture defined not by individual tools but by coordinated autonomy.

Autonomous SOC operations deliver faster containment, automated triage and continuous defense. They do not replace analysts; they remove bottlenecks that used to slow them down. Importantly they also shrink the window in which adversaries can influence citizens or target youth offering cognitive protection through operational speed. Canada cannot rely on incremental improvements. The risks are here, the tempo is rising and adversaries are accelerating. Autonomous SOC operations are not an optional enhancement as they are a strategic national requirement.

Looking ahead toward 2026 one prediction becomes clear. The coming year will mark the operationalization of agentic AI at scale, but it will also introduce the rise of AI World Models systems capable of orchestrating dreaming machines that operate one layer above agentic AI. These models will allow society to simulate, reason and act with a new form of coordinated intelligence. In this environment a pragmatic risk approach will be essential for guiding adoption, securing systems and ensuring that human purpose remains at the center of technological progress.

Agentic AI marks a national inflection point. Foreign interference is expanding. Youth radicalization risks are escalating. The 5D model is already in motion. Canada must not freeze. Canada must fortify. And Canada must ensure that humans, our judgment, our ethics, and our purpose remain the ones steering the intelligence we create.

Darwin Tusarma is an ethical hacker and penetration tester with over twelve years of experience applying offense informed defense to protect enterprise and industrial OT environments in Canada.

Diego Ramirez is Senior Manager of the Cyber Intelligence Centre at Bell Cyber leading advanced security operations focused on autonomous SOCs automation and OT cyber defense.

Rafael Ramírez is a cybersecurity leader with over twenty years of experience focused on resilience, trust and execution as founder of TruNorth CyberSphere.

A Data Driven View: The Canadian Cybersecurity Landscape

by Richard Stiennon

Canada is home to 140 cybersecurity vendors. From the established giant roll-up which is OpenText to the 2025 AI Security startups AllTrue and Identity Machines, the Canadian cyber ecosystem bears more similarity to US and Israel than the UK and Germany. The top 16 countries ranked by number of vendors are found in Table 1.

There is a marked difference between the make up of US and Israeli cyber companies and those of the rest of the world. There is strong support from the venture capital community for startups in those two countries. In the UK and Germany there is much less support for startups. Both German and UK startups are typically bootstrapped or have support from a parent company or large customer. There is little attempt to create products that will sell worldwide or compete directly with foreign vendors. The UK can be characterized by hyper-local companies that serve just the surrounding community.

Table 1

Country	# of Vendors
USA	2054
Israel	273
United Kingdom	266
Germany	141
Canada	140
France	105
India	91
Australia	72
Switzerland	64
Netherlands	49
Singapore	42
South Korea	41
Spain	40
Ireland	34
Sweden	33
Poland	31

Canada, on the other hand, most resembles the United States, albeit at a smaller scale. It has a history of disruptive cybersecurity companies that have had a global impact. It has the giant US market to easily sell into. It also has pockets of innovation, most notably the Waterloo, Ontario area that came to prominence during the mis-guided US ITAR rules of the '90s that locked down the market for free and open access to encryption technology. The University of Waterloo was the beneficiary of that failed policy decision and to this day is known for its programs in encryption. It also serves as a feeder of qualified candidates to startups like eSentire, a managed detection and response company headquartered in neighboring

Cambridge. eSentire has hired 606 people across all its operations. Two of the largest Canadian tech companies, OpenText, and Blackberry, are in Waterloo.

Ottawa is also at the center of a cybersecurity enclave of 12 companies. Canada's largest networking companies, Nortel Networks and Newbridge Networks were headquartered in Ottawa. When demand for security took off at the end of the last century there were Canadian companies founded by eterans of these networking giants. Entrust Technologies was spun out of Nortel to commercialize its encryption and PKI software in 1996. Third Brigade, an endpoint security company based in Ottawa was acquired by Trend Micro in 2009. Many of its executives assumed leadership roles within Trend that they still hold today.

Table 1-1

City	# of Vendors
Toronto	40
Montreal	14
Vancouver	12
Ottawa	12
Mississauga	10
Waterloo	7
Kitchener	5
Calgary	4
Victoria	3
Québec	3

Table 1-2

Category	# of Vendors
Data Security	29
IAM	28
GRC	16
Network Security	13
AI Security	8
Endpoint Security	8
MSSP	8
Application Security	6
Email Security	6
Operations	5
IoT Security	4
Threat Intelligence	4
Security Analytics	2
API Security	1
Fraud Prevention	1
Training	1

Toronto is home to 40 cybersecurity vendors, 50 if you count Mississauga's ten. See Table 1-1 for more details.

Canada has cybersecurity vendors in 16 categories, see Table 1-2 for a detailed breakdown.

The prominence of Data Security vendors can be attributed to the impact of the success of Entrust as well as the University of Waterloo graduates. Note that GRC is third in Canada whereas it dominates in the US.

Two of the fastest growing cybersecurity companies are:

Tailscale provides secure networking solutions through a WireGuard-based virtual private network that creates point-to-point connectivity between devices and enforces

Chart 1: Tailscale Headcount Growth

252 Employees

3.2% Recent Growth

2021	2022	2023	2024	2025
3.45%	108.57%	48.75%	20.97%	49.7%

least privilege access principles. It has grown 50% in headcount in 2025 to 252 employees, see Chart 1 for details. It has taken in a total of US $288.67 million investor backing. George Kurtz, the CEO of Crowdstrike participated in its $173 million Series C round in April 2025.

AllTrue.AI is one of eight AI Security startups in Canada. It is also one of the fastest growing by headcount in 2025. It is up 89% with 34 employees. The company's primary solution is the TRiSM Hub, which automates the discovery, cataloging, and real-time monitoring of all AI assets within an organization including models, pipelines, applications, and systems.

Investments

Over the years, the 66 funded vendors we track have taken in a total of US $2.65 billion. See Table 1-3 for the top 16 vendors by funding level.

1Password is notable for its high funding level for its password management solutions. The make up of its investors is also interesting. In addition to VC firms like Jeffrey Katzenberg's WndrCo, there are many well known names on its cap table. Scarlett Johansson, Ryan Reynolds, Ashton Kutcher, Robert Downey Jr., Justin Timberlake, and Matthew McConaughey are all backers.

Vancouver based **Trulioo** is also in the identity space but delivers an identity verification platform that integrates Know Your Customer, Know Your Business, and anti-money laundering functionalities.

Field Effect Software is a Managed Detection and Response platform vendor out of Ottawa. It provides the software that Managed Service Providers use to provide security monitoring and alerting services.

Mode develops specialized platforms for secure, out-of-band communication during cyber incidents, focusing on maintaining operational continuity when primary systems are compromised. While not always cybersecurity related, out-of-band comms are often crucial during ongoing cyber attacks.

Corsa specializes in providing a comprehensive system for network security virtualization designed primarily for large-scale environments. Their core capability centers on enabling organizations to replace conventional physical firewall appliances with virtualized alternatives deployed across standardized server infrastructures. Through their proprietary orchestrator platform, they deliver unified oversight and administration of distributed virtual firewall instances operating throughout complex networks.

Note that funding for **Magnet Forensics** in Waterloo is not recorded but the company was acquired by Thoma Bravo in 2023. The company develops digital investigation solutions that acquire, analyze, report on, and manage evidence from digital

Table 1-3

Name	Category	City	Founding Year	Total Funding*	Funding in 2025*	% Growth in 2025	Current Headcount
1Password	IAM	Toronto	2005	920.14	0	12.49	2809
Trulioo	IAM	Vancouver	2011	474.96	0	-3.34	376
Tailscale	Network Security	Toronto	2019	288.67	173.67	50.9	252
eSentire	MSSP	Cambridge	2001	184.07	0	2.54	606
Field Effect Software	MSSP	Ottawa	2016	88.11	0	-3.9	148
Mode	Data Security	Calgary	2022	80.99	0	-68	8
Corsa	Network Security	Ottawa	2011	50.7	0	-12	22
integrate.ai	AI Security	Toronto	2017	49.23	0	-11.43	31
Ethoca	Fraud Prevention	Toronto	2005	44.74	0	5.68	186
Flare	Operations	Montreal	2017	40.47	0	29.09	142
ISARA	Data Security	Waterloo	2015	26.94	0	9.52	23
Qohash	GRC	Quebec	2018	25.15	0	16.95	69
Absolute Software	Endpoint Security	Vancouver	1993	24.55	0	7.54	1227
BOXX Insurance	GRC	Toronto	2018	23.99	0	6.78	63
Hyas	Threat Intelligence	Victoria	2015	23.8	0	-7.69	24
GoSecure	MSSP	Montreal	2002	23.45	0	-4.09	164

*Millions of USD

sources including mobile devices, computers, IoT devices, and cloud services. Thoma Bravo is the biggest acquirer of cybersecurity companies. It has always had close ties to the Ontario Teachers' Pension Plan which participates in many Thoma Bravo investments.

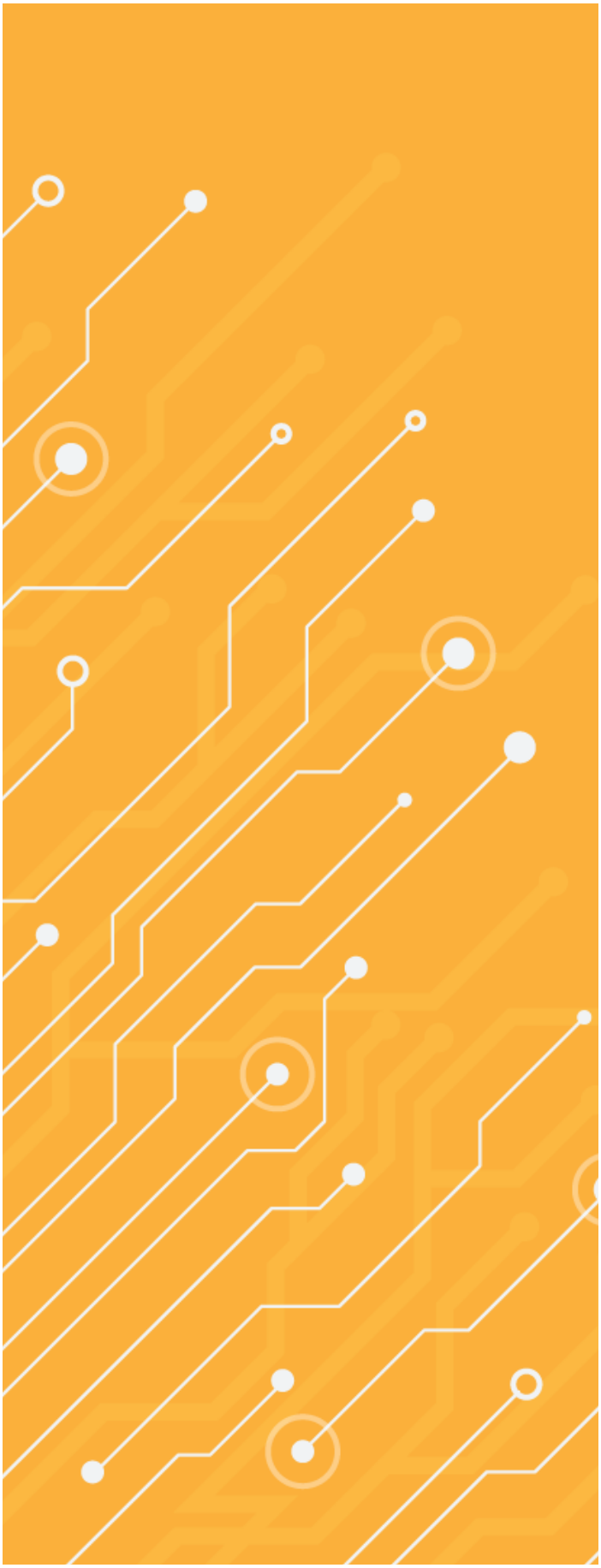
Canada is poised for growth in cyber

Canada has earned its place in the top five countries for cybersecurity innovation thanks to both its history in the telecom business as well as its academic centers that produce technology experts. As large vendors like **1Password** and **OpenText** continue to grow and demonstrate successful outcomes the Canadian market will grow in appeal to venture capitalists.

Adding to the short list of public Canadian cyber companies (**Cybeats** and **Plurilock**) will enhance the perception of the cyber eco-system in Canada. That, and successful exits will have a positive impact because it will create more entrepreneurs and investors that have an appetite for cybersecurity startups.

Canada also has the advantage of being the closest neighbor to the United States during a time of internal strife that has created a hostile environment for immigrants, students, and the outspoken. Providing a safe haven for inventors, entrepreneurs, and capital will ensure that Canada continues to grow its contribution to the overall cybersecurity industry.

Richard Stiennon is Chief Research Analyst for IT-Harvest, the firm he founded in 2005 to cover the 4,070+ vendors that make up the IT security industry. He has presented on the topic of cybersecurity in 32 countries on six continents. He was a lecturer at Charles Sturt University in Australia. He is the author of *Surviving Cyberwar* (Bloomsbury, 2010) and Washington Post Best Seller, *There Will Be Cyberwar*. His research appears on Substack. Stiennon was the Chief Marketing Officer for Fortinet, Inc. and VP Threat Research at Webroot Software. Prior to that he was VP Research at Gartner. He has a B.S. in Aerospace Engineering from the University of Michigan, and his MA in War in the Modern World from King's College, London. His latest book, *Guardians of the Machine Age: Why AI Security Will Define the Future of Digital Defense* is coming out in early 2026.



The Power of Collaboration

by Jennifer Quaid

In an age where digital systems underpin nearly every aspect of society, we need to rethink our relationship with security. We can't afford to view cyber security as an internal function of an organization, best maintained in secret. Silence is the enemy of good cybersecurity because it allows threats to spread unchecked and prevents organizations from learning from each other's experiences. When an organization conceals information about an attack, others lose the opportunity to prepare for similar attacks. Cyber attackers exploit this silence. They rely on the fact that victims are not sharing indicators of compromise, new vulnerabilities, or attack methods. As a result, the same tactics can and will be reused across multiple targets.

Threat actors are cooperating to operate across borders, industries, and technologies, exploiting every opportunity. We give them those opportunities when we fail to share information. Collaboration is now one of the most critical components of effective cybersecurity. It strengthens collective defense, accelerates incident response, and raises the overall resilience of national and global digital ecosystems.

Increasingly, cyber threats spread beyond an organization or a sector. Malware campaigns, supply-chain attacks, and ransomware are frequently spread through shared vendors, interconnected networks, or common software platforms. The 2020 SolarWinds attack is a perfect example, the compromise of a widely used IT management tool allowed

Collaboration Enables:

Improved resilience: Sharing best practices enables organizations to develop understanding, policies and practices that will help them to be more resilient.

Faster detection and response: Sharing knowledge of attackers' techniques lets others proactively scan networks and patch before attacks spread.

Supply-chain and third-party risk awareness: Many breaches stem from shared infrastructure (cloud identity, remote access portals, or software dependencies). Shared threat data would help organizations identify which components are under active threat and proactively defend themselves.

Cross-sector protection: Healthcare systems, airlines, retail and entertainment platforms all occupy different sectors, yet attackers are using the same techniques against all of them. When all sectors share information, no industry is left isolated.

attackers to infiltrate numerous government agencies and private companies. A single organization acting alone could not have detected or mitigated such a widespread threat. Instead, collaborating between public-sector cybersecurity agencies, private cybersecurity firms, and affected organizations helped to identify the breach, understand how it worked, and deploy appropriate measures.

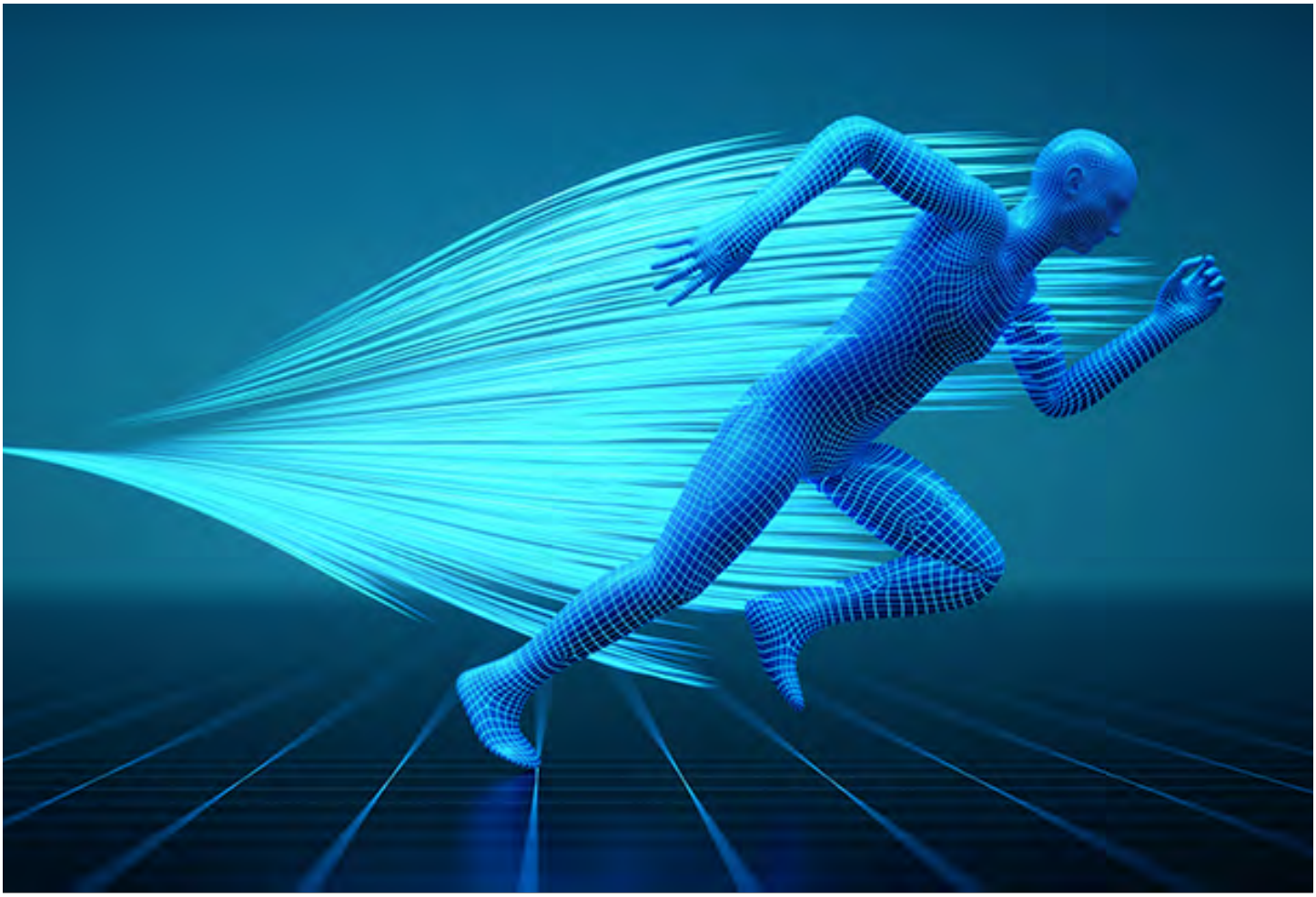
Collaboration enables more accurate and timely threat intelligence sharing, raising the resilience for all. Many organizations hesitate to disclose attack information, yet the sooner others know about a new tactic or vulnerability, the faster they can protect themselves. Generally, organizations with strong information-sharing practices are more resilient because they have the opportunity to transform isolated incidents into collective insight. They leverage facilitated real-time information sharing which enables them to collectively defend themselves. They are stronger, together.

Another area where collaboration makes a difference is in the better understanding of effective practices and procedures, shared standards and best practices. Cybersecurity is complex and constantly evolving, even the best resourced organizations struggle to keep up with the ever-changing threats. By partnering with peers, organizations can collectively develop a better understanding of the threats and mitigations and create guidelines that benefit the entire ecosystem.

Finally, silence erodes trust and trust is at the foundation of security. Collaboration and sharing strengthens our collective defense: the more openly organizations communicate about threats, the harder it becomes for attackers to succeed. Collaboration builds trust. Cybersecurity is not merely a technical challenge, it is about people. As cyber threats continue to escalate in scale and sophistication, trust-driven cooperation will be essential.

Cross-sector collaboration is no longer optional. It is the foundation of a resilient digital society. By sharing information, experiences and best practices, organizations across sectors can collectively raise the bar of cybersecurity and better defend against threats that no single organization could withstand alone. If knowledge is power, collaboration is the force-multiplier, and silence is the enemy of good cyber security.

Jennifer Quaid is the Executive Director of the Canadian Cyber Threat Exchange (CCTX), Canada's preeminent private sector organization for cross-sector collaboration, enabling cyber resilience and preparedness in its members. She is responsible for advancing the mission and purpose of the CCTX and delivering value to the membership.



The Global Race for Cybersecurity and Innovation

by François Guay

How smaller nations are surging ahead and what Canada must do now to compete and lead

Canada is at an inflection point. The global cybersecurity landscape is shifting faster than at any time in the last decade. Artificial intelligence is amplifying threats. Nation state cyber operations are intensifying. Cyber-crime networks are multiplying. Yet at the very moment the world is accelerating, Canada is struggling to keep pace in the two areas that matter most for national competitiveness: cybersecurity capacity and innovation output.

This is not because Canada lacks talent or resources. It is because other nations, many of them far smaller, have found ways to concentrate strategy, capital, policy, and industry partnerships with an intensity Canada has not yet matched.

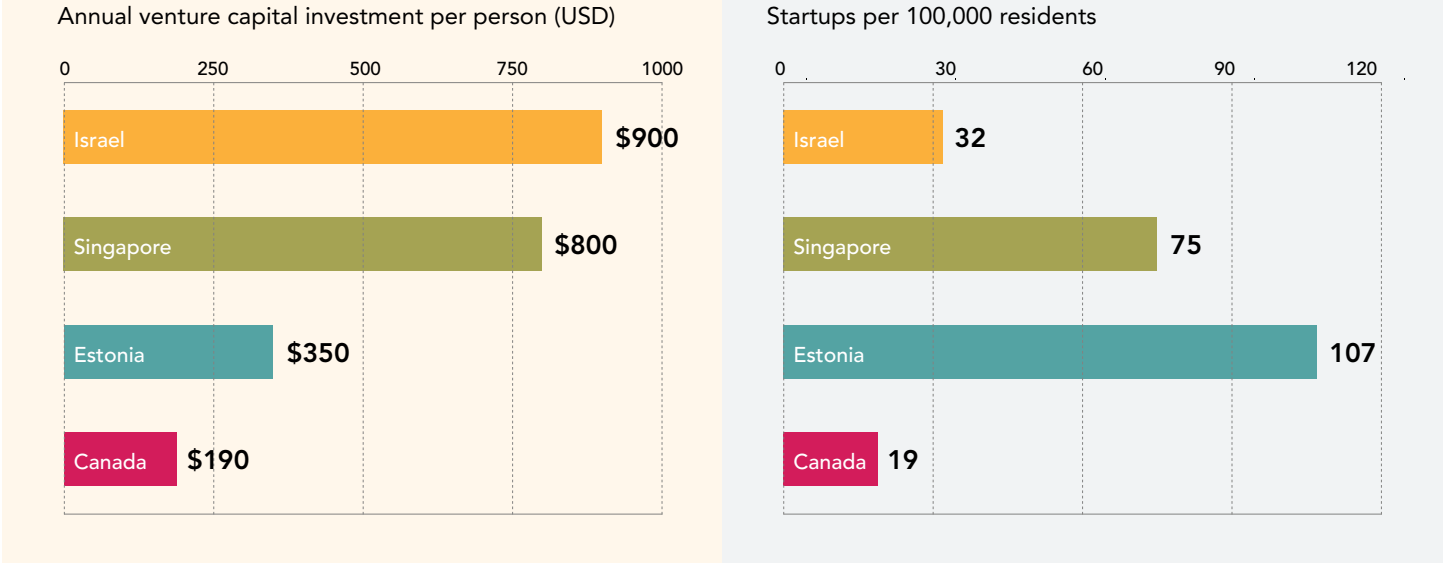
A comparison with three standout innovation and cybersecurity economies Israel, Singapore, and Estonia reveals a striking pattern. Each of these countries has built global leadership not through scale but through focus. Their success proves that country size does not determine competitiveness, strategy does.

Canada has the building blocks. What it does next will determine whether it emerges as a global cybersecurity leader or continues to watch smaller nations achieve disproportionate gains.

The Competitiveness Gap

A review of key indicators reveals a consistent story. Canada performs well globally but falls behind when measured per person and when the comparison is limited to top tier innovation nations.

Canada Has Scale. Others Have Intensity.



Population and Economic Scale

Canada has almost 40 million people. Israel has 10 million. Singapore has 6 million. Estonia has fewer than 1.4 million. Yet all three smaller nations are outperforming Canada in startup creation, innovation velocity, venture capital, and cyber readiness.

Startups Per Capita

Canada has about 7,200 startups, or 19 startups per 100,000 residents. Israel has about 6,000 startups and the highest startup density in the world, roughly 32 per 100,000 people. Estonia has about 1,500 startups, an extraordinary number given its population. Singapore has about 4,500 startups and is the gravitational center for Southeast Asian venture investment.

Unicorn Count

Canada has about 30 unicorns. Israel has about 100, and many of them are cyber companies. Estonia has 10 unicorns, the most per capita in the world. Singapore has roughly 30.

Venture Capital Per Capita

Canada sees about $7.9 billion of annual venture investment, equal to roughly $190 per person. Israel invests about $9 to 10 billion annually, which equals more than $900 per person. Singapore invests nearly $800 per person. Estonia invests about $350 per person and leads the world relative to GDP at more than 1.1 percent of national output.

Exits and Ecosystem Maturity

Canadian tech exits totaled about $5.2 billion across 40 deals in 2024. Israel generated $70 billion in exits in the first 11 months of 2025 alone, including the $32 billion acquisition of Wiz. Singapore has produced some of Southeast Asia's largest public offerings, including Grab's $40 billion debut. Estonia produced Skype and continues to see strong acquisition activity relative to its size.

Cyber Readiness

Singapore ranks near the top of global cybersecurity indices. Estonia is recognized globally for resilience and innovation in digital governance. Canada performs well but sits outside the global top ten despite a much larger economy and federal cyber investment like peer nations. The pattern is clear. Canada is strong, but not strong enough relative to what the world's leaders are doing.

Three Models that are Winning

Canada's gap is not accidental. It reflects deliberate choices other countries have made. Three models stand out.

1. Israel Defence Driven Commercial Innovation

Israel has blurred the line between national security, cyber capability, and commercial innovation. Elite cyber talent develops inside the defense ecosystem then flows into the private sector. Venture capital follows talent. Universities, government,

and capital markets operate in alignment. The result is a continuous pipeline of cyber startup creation unmatched anywhere in the world.

KEY FEATURES

- Early identification of technical talent
- Compulsory service that accelerates real world experience
- Government funding and procurement that boosts commercialization
- Strong global capital attraction

2. Singapore State Supported Global Talent Hub

Singapore is small but intentional. It invests aggressively in digital readiness, national cybersecurity infrastructure, and targeted innovation sectors. It pursues global talent rather than focusing solely on domestic pipelines. Its agency model for innovation and cyber gives it a level of coordination and speed most countries cannot match.

KEY FEATURES

- Significant multiyear national cybersecurity funding
- A strong global workforce policy
- A focus on commercialization and scale across Southeast Asia
- Pro-business regulatory strategy that accelerates growth

3. Estonia Digital First National Architecture

Estonia transformed itself after regaining independence by building a digital government from the ground up. Digital identity, online voting, secure data exchange systems, and cyber infrastructure are all foundational. These investments created trust and efficiency and attracted global innovators. Its lean lightweight government model makes rapid change possible.

KEY FEATURES

- Nationwide digital identification
- Interoperable cyber secure public infrastructure
- Startup visas and pro innovation immigration flows
- Cultural embrace of digital experimentation

Each of these countries made strategic choices Canada has not yet made at scale.

The Canadian Challenge: Not Yet Designed for Speed or Scale

Canada has world class universities, globally respected cyber researchers, a strong banking sector, and a growing base of cyber talent. Yet Canada lags because two structural barriers remain unaddressed.

FRAGMENTED NATIONAL STRATEGY

Canada has many excellent programs but lacks an integrated overarching plan like national models in Singapore or Israel. Efforts remain siloed across provinces, agencies, ministries, and sectors.

CHRONIC COMMERCIALIZATION GAP

Canada produces talent and research but struggles to convert both into successful startups and large scale exits. Lack of risk capital, low incentives for patient capital, slower adoption by enterprise buyers, and regulatory uncertainty all slow down commercialization. These challenges are solvable, but not without a decisive shift.

A Blueprint for Becoming a Global Cybersecurity and Innovation Powerhouse

Canada does not need to copy any country. It needs to study what works and adapt it to Canadian strengths. The following actions represent high impact strategic steps.

1. Build a Canadian Cyber Talent Accelerator Modeled on Global Best Practice

Canada should create a national cyber talent accelerator that identifies and develops high potential technical talent as early as high school and guides them through a structured program combining hands-on learning, work integrated experience, and industry mentorship. The accelerator should partner with academic institutions, provinces, and industry, and include fast track pathways for advanced learners like Israel's Unit eighty-two style model but tailored to Canadian values.

2. Launch a Cybersecurity Commercialization Fund Focused on Scaling Canadian Startups

Canada's startup creation numbers are solid. What is missing is aggressive commercialization early on. A national cyber commercialization fund with risk sharing mechanisms like Singapore's corporate partnership model would help bring Canadian products to market faster. Funding should be paired with procurement incentives within government and critical infrastructure.

3. Create a National Cyber Cluster Strategy

Israel has Beersheba. Singapore has its one north innovation district. Estonia has its integrated digital society. Canada has many clusters but no unified cyber corridor. A national strategy linking Calgary energy firms, Ottawa's defense and public sector ecosystem, Toronto's fintech concentration, Montreal's AI leadership, and Vancouver's startup community would create a unique competitive advantage.

4. Attract Global Cyber Talent and Companies to Canada

Canada should build an express pathway for global cybersecurity professionals like Estonia's startup visa or Singapore's tech pass. Canada can also become the safest and most strategically located global headquarters for cyber firms wanting a presence in North America.

5. Accelerate Enterprise Adoption of Canadian Cyber Technologies

Large organizations in Canada adopt domestic technology more slowly than global competitors. A made in Canada cybersecurity adoption initiative with incentives for enterprises would dramatically improve the commercialization landscape.

6. Invest in Public Cyber Readiness at the Scale of Global Leaders

Canada's per capita cyber spending is comparable to the United States but still trails Singapore and likely Israel when military cyber budgets are included. With increasing national exposure to AI driven threats, investment must rise and be paired with a unified national architecture and clear accountability.

Why This Matters: Canada Has a Narrow Window to Lead or Lag

Countries like Israel, Singapore, and Estonia show what is possible when vision, policy, and capital align. Their success is not accidental. It is engineered. Canada has more people, a larger economy, deeper academic institutions, and one of the most diverse talent pools in the world. Canada should be a global cyber superpower. It can get there, but not by relying on incremental change.

The moment to choose ambition is now. The next decade will redefine national digital strength. Canada can compete with the world's best if it commits to bold strategy at the speed the global cybersecurity landscape demands.

See end notes for this article's references.

François Guay is the visionary founder of the Canadian Cybersecurity Network (CCN), Canada's largest cybersecurity community, bringing together more than 46,000 members and reaching over one million and a half Canadians through its extended network of companies, universities, professional associations, and government partners.

Conclusion & Recommendations

Canada's cybersecurity challenge in 2026 is no longer defined by isolated breaches or purely technical failures, but by sustained pressure on trust, identity, resilience, and human decision making. Across every domain examined in this report, from AI enabled fraud and deepfake impersonation to crisis readiness, cyber insurance convergence, agentic AI, and post quantum cryptography, a consistent reality emerges. The threat landscape is accelerating faster than traditional security models, governance structures, and assumptions were designed to handle.

The most consequential shift is not technological, but conceptual. Cyber risk has moved beyond the perimeter, beyond infrastructure, and into human trust, identity assurance, and leadership response under pressure. Attackers no longer need to break systems when they can manipulate people, exploit urgency, and weaponize familiarity. Deepfakes, voice cloning, and AI driven social engineering have rendered visual and auditory confirmation unreliable, eroding long held assumptions about how trust is established. At the same time, harvested data, legacy cryptography, and immature post quantum readiness mean that today's decisions will determine tomorrow's exposure.

This report also makes clear that preparedness, not intent, separates resilient organizations from those that fail under pressure. Many institutions believe they are ready, yet tabletop exercises, real world incidents, and insurance claims consistently reveal gaps in authority, coordination, communications, and execution. Cyber incidents have become full scale business crises, where early decisions shape operational continuity, regulatory outcomes, financial loss, and long term reputation. In this environment, resilience is built before an incident occurs, not during it.

Canada's position is neither fragile nor complacent. The country benefits from strong talent, credible innovation, and a growing cybersecurity ecosystem capable of global impact. However, resilience remains uneven, particularly among small and mid sized organizations, operational technology environments, and identity centric processes. Closing these gaps will require moving beyond incremental improvements toward systemic change, including verifiable identity, zero trust assumptions across all channels, practiced crisis leadership, and closer integration between cybersecurity, insurance, and governance.

The path forward is clear. Canada must continue shifting from reactive defense to proactive resilience, from implied trust to verified trust, and from siloed controls to coordinated ecosystems.

Leadership must treat cybersecurity as a discipline of preparedness, judgment, and accountability, not a technical function delegated downward. The risks are already present, the tempo is rising, and the cost of delay is compounding.

Canada does not need to be louder or more aggressive. It needs to be deliberate, prepared, and resolute. The posture required for 2026 is one of calm strength, grounded awareness, and the readiness to defend digital space, economic stability, and public trust when it matters most.

TOPIC

Cyber Resilience and Risk Management

TITLE

Strengthening Canada's Cyber Resilience: Key Insights and Recommendations

AUTHOR

Amisha Parikh

SIGNALS

- Legacy systems, identity fraud, and AI-driven attacks are top vulnerabilities
- Collaborative models improve detection, response, and intelligence
- SMEs need tools and guidance to raise baseline security
- AI automation with human oversight critical for proactive defense

TOPIC

Insider Risk and Security Culture

TITLE

The Human Factor of Risk: Understanding Insider Threats

AUTHOR

Lina Dabit

SIGNALS

- Most insider incidents are unintentional
- Shadow AI creates visibility blind spots
- Security culture must empower, not punish
- Human awareness remains the first control

TOPIC

Deepfake and AI-Powered Social Engineering Threats

TITLE

The New Face of Fraud: How Deepfakes Are Breaching Your Perimeter

AUTHOR

Tracey Nyholt

SIGNALS

- Generative AI enables realistic audio/video deepfakes
- Employee trust in voices/faces increasingly unreliable
- Caller ID, security questions, and voice recognition insufficient
- Out-of-band authentication and ITSM integration harden defenses

TOPIC

Data Governance, Classification and Security

TITLE

Stop (Only) Securing the Perimeter: Your Data is Exposed, and You Don't Know Where to Look

AUTHOR

Jaap Mantel

SIGNALS

- Perimeter security alone is insufficient
- Legacy tools create false positives and missed risks
- AI and multi-factor classification improve accuracy
- Data remediation needs human oversight
- Resilience comes from governing critical data

TOPIC

AI's Impact on Canadian Cybersecurity

TITLE

Ten Insights into How AI Is Reshaping Cybersecurity in Canada

AUTHOR

David Masson

SIGNALS

- AI boosts phishing, malware, and targeted attacks
- Readiness to defend against AI threats is low
- AI excels at anomaly detection but underused
- Managed security services preferred due to skills gaps
- Governance, data privacy, and cautious autonomy are key

TOPIC

Deepfake and AI-Powered Social Engineering Threats

TITLE

How Leadership Decisions Make Cyber Breaches More Expensive

AUTHOR

Mary Carmichael

SIGNALS

- Breach costs are set before the incident occurs
- Cyber insurance reduces shock, not exposure
- Vendor concentration amplifies financial risk
- Governance decisions drive recovery outcomes

TOPIC

Cyber Crisis Simulation and Preparedness

TITLE

Facilitating Cyber Crisis Tabletop Exercises: Insights from the Front Line of Simulation Leadership

AUTHOR

Simon Hodgkinson

SIGNALS

- Tabletop exercises reveal gaps in people, processes, and tech
- Focus on business resilience, not just technical response
- Challenges: varying preparedness, decision paralysis, overreliance on tech, assumptions about systems
- Debriefs and pre-approved protocols improve continuity

TOPIC

Post Quantum Cryptography Transition

TITLE

Post-Quantum Cryptography (PQC): The Looming Cryptographic Shift

AUTHOR

Munis Badar

SIGNALS

- Harvest-now-decrypt-later attacks already happening
- PQC migration requires global coordination
- Hybrid certificates are a bridge, not an endpoint
- Crypto agility must be designed, not retrofitted

TOPIC

Cyber Insurance and Security Integration

TITLE

Converging Paths: Where Cyber Insurance and Security Intersect

AUTHOR

Jonathan Weekes

SIGNALS

- Cyber insurance shifting from reimbursement to prevention
- Collaboration between insurers, vendors, SMEs strengthens defense
- Continuous monitoring reduces incidents and downtime
- Integrated approach raises security baseline and aligns risk

TOPIC

Cyber Resilience and Regulatory Change

TITLE

2025: The Year Cybersecurity Became a Systemic Resilience Mandate

AUTHOR

Femi Ogunji

SIGNALS

- Cybersecurity shifted from prevention to resilience
- Cybercrime scaled into enterprise-grade threats
- Supply chain and human vulnerabilities drove systemic risk
- Regulation (DORA) forced resilience into board-level focus
- Zero Trust and XDR became essential foundations

TOPIC

Critical Infrastructure and Cyber Resilience

TITLE

Securing Critical Infrastructure: Canada Can Light the Way Forward

AUTHOR

Cheryl Biswas

SIGNALS

- Critical infrastructure underpins security and economy
- Cyber, climate, and geopolitical risks are converging
- IT exposure increases OT and infrastructure vulnerability
- Data residency ≠ data sovereignty
- Resilience depends on collaboration, not regulation alone

TOPIC

Human Factor and AI-Enhanced Social Engineering

TITLE

It Was Bad in 2018 — It's Worse Now

AUTHOR

Scott Augenbaum

SIGNALS

- Most cybercrime preventable with awareness and behavior
- AI amplifies social engineering attacks
- Victims fall prey due to trust, urgency, or mindset
- Cybersecure Mindset framework teaches prevention habits

TOPIC

Workforce and National Resilience

TITLE

Canada's Cyber Talent Pipeline Under Strain

AUTHOR

James Cairns

SIGNALS

- Canada's cyber talent pipeline is shrinking
- AI increases demand for human oversight
- Entry-level pathways are breaking
- Workforce resilience is national security

TOPIC

Cyber Leadership and Resilience

TITLE

The Future of Cyber Leadership: The Rise of the Post Breach CISO

AUTHOR

Michelle Balderson

SIGNALS

- Assume compromise and design for resilience
- Security decisions must support operations
- IT and OT security cannot remain separated
- Leadership context matters as much as controls

TOPIC

AI Security and Agentic Workflows

TITLE

Model Egress: The New Security Perimeter No One Is Monitoring

AUTHOR

Jason Keirstead

SIGNALS

- Agentic AI creates "shadow agents" inside networks
- Firewalls/EDRs blind to AI-driven outbound flows
- Risks include prompt injection, data exfiltration, runaway processes
- Call Graph monitoring and SPIFFE enable real-time governance
- Security must shift from network to semantic runtime visibility

TOPIC

Collective Cyber Defense

TITLE

The Power of Collaboration

AUTHOR

Jennifer Quaid

SIGNALS

- Sharing raises resilience across sectors
- Supply chain risk requires shared visibility
- Trust is a security control

TOPIC

Cyber Leadership and Resilience

TITLE

The Global Race for Cybersecurity and Innovation

AUTHOR

François Guay

SIGNALS

- Cyber leadership is built through focus, not size
- Fragmented strategy slows national competitiveness
- Talent without commercialization limits global impact
- Speed and coordination outperform scale
- Cybersecurity strength is economic power

References

The New Face of Fraud: How Deepfakes Are Breaching Your Perimeter by Tracey Nyholt, Presented by TechJutsu

Web Articles:

CNN. "Finance worker pays out $25 million after video call with deep-fake 'CFO'." CNN Business, February 4, 2024.

WSJ. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case." The Wall Street Journal, August 30, 2019.

FBI. Internet Crime Report 2023. Washington, D.C.: FBI, 2023. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Federal Trade Commission. "Chatbots, deepfakes, and voice clones: AI deception for sale." FTC Consumer Advice, March 20, 2023. h

NIST. Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Galluzzo R, Richer JP (2025) Digital Identity Guidelines: Authentication and Authenticator Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63B-4.

2025: The Year Cybersecurity Became a Systemic Resilience Mandate by Femi Ogunji

Books, Reports, and Industry Studies

Cybersecurity Ventures. "Cybercrime Magazine Annual Report: The Official Annual Cybercrime Report." Report, 2025.

European Union. *Digital Operational Resilience Act (DORA).* Official Journal of the European Union, January 17, 2025.

European Union. *Cyber Resilience Act (CRA).* Proposed Regulation, various provisions set for 2026 enforcement.

Forrester Research. "The State of Zero Trust Security." Annual Report, 2025.

Gartner. "Market Guide for Extended Detection and Response (XDR)." Annual Analysis, 2025.

Group-IB. "Annual High-Tech Crime Trends Report." Threat Intelligence Analysis, 2025.

ISC2. "Cybersecurity Workforce Study." Annual Report, 2025.

National Institute of Standards and Technology (NIST). "Post-Quantum Cryptography Standardization Process." Ongoing Program Status, 2025.

Palo Alto Networks. "The Cyber Security Skills Gap: Driving Strategic Automation." Thought Leadership Paper, 2024.

Sophos. "The State of Ransomware Report." Annual Survey, 2025.

U.S. Bureau of Labour Statistics. "Occupational Outlook Handbook: Information Security Analysts." Annual Projections.

U.S. Citizenship and Immigration Services (U.S.CIS). "H-1B Cap Season: Annual Statistical Report."

World Economic Forum (WEF). "Global Cybersecurity Outlook." Annual Report, 2026.

News and Industry Publications

Ars Technica. "High-Impact Vulnerability in Oracle E-Business Suite Exploited by Clop Group." September 2025.

Axios. "DoorDash Targeted by Social Engineering Attack, Customer Data Exposed." November 2025.

Dark Reading. "The Rise of Agentic AI: New Defence Strategies for Autonomous Attacks." January 2026.

The Financial Times. "Cyber Insurance Premiums Soar as Insurers Demand Stricter MFA and EDR Controls." March 2026.

Wired. "The Fourth Pillar: Why Authenticity Must Join CIA." Opinion Editorial, December 2025.

Government and Non-Profit Organizations

CISA (Cybersecurity and Infrastructure Security Agency). "Threat Forecast: Critical Infrastructure and Operational Technology." Intelligence Bulletin, 2026.

FSB (Financial Stability Board). "Report on Cyber Resilience in the Financial Sector." International Policy Paper, 2025.

Securing Critical Infrastructure by Cheryl Biswas

Bisson, Neil. "How the CSOS Director's Annual Speech Frames Today's Sabotage and Proxy Threats." Substack. November 14, 2025.

Dabit, Lina. "Canada Under Pressure: Navigating the Hybrid Threat Landscape." Wired for Change podcast.

BC Cyber Hub Pilot Project: Strengthening Cybersecurity Resilience.

Department of Finance Canada. "Canada Strong Budget 2025." https://budget.canada.ca/2025/home-accueil-en.html

Greer, Deryck. "Strengthening Cybersecurity in Canada's Public

References

Sector: Key Insights and Strategic Recommendations." The State of Cybersecurity in Canada 2025.

Dubé, David. "Firewalls and Frontlines: Canada's Cybersecurity Leadership Potential in the Age of Foreign Information Operations." Network for Strategic Analysis.

Lawrence, Mark. "Wait … Who Owns Our Data? Why the U.S. May Access Information Stored on Canadian Soil – and What We Should do About it" LinkedIn Pulse. December 16 2025

Miller, Gabriel. "21st Century Defence Science Cyber Engineering and Tech Experts Will Defend our Sovereignty" Universities Canada. November 27, 2025.

Public Safety Canada. "Parliamentary Committee Notes: Cybersecurity and Protecting Canada's Critical Infrastructure." March 2025.

Chery Biswas and James Troutman, presenters. "Do You Want to Play A Game? How About Disabling Civilization" BSides Ottawa Policy Village November 2025.

Shelly Bruce, Don Costello, and Earl Maynard, presenters. "The BC Cyber Hub Pilot Project

Canada's Cyber Talent Pipeline Under Strain by James Cairns

Canadian Centre for Cyber Security. 2024. Cyber Threat Bulletins. Ottawa: Communications Security Establishment.

Colleges and Institutes Canada. 2023. International Students in Canada's Colleges and Institutes: 2023 Data Report. Ottawa: CICan.

Immigration, Refugees and Citizenship Canada (IRCC). 2024. Canada Introduces Intake Cap on International Student Permit Applications. Ottawa: Government of Canada.

IRCC. 2024b. Post-Graduation Work Permit Program (PGWPP) Changes. Ottawa: Government of Canada. https://www.canada.ca/en/immigration-refugees-citizenship/services/study-canada/work/after-graduation.html

IRCC. 2024c. IRCC Statistical Reports and Data Tables: Study Permit Approval and Processing Rates. Ottawa: Government of Canada.

IRCC. 2024d. Check Processing Times – Study Permit (Outside Canada). Government of Canada.

IRCC. 2026. Supplementary Information for the 2026-2028 Immigration Levels Plan. Ottawa: Government of Canada.

ISC2. 2024. Cybersecurity Workforce Study: 2024 Global Findings. Alexandria, VA: ISC2.

Organisation for Economic Co-operation and Development (OECD. 2022). OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. Paris: OECD Publishing.

Organisation for Economic Co-operation and Development (OECD. 2023). Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States. OECD Skills Studies. Paris: OECD Publishing.

Organisation for Economic Co-operation and Development (OECD. 2024). Digital Security (Policy-Issues Series). Paris: OECD Publishing.

Statistics Canada. 2025. Job Vacancies, Labour Force Survey: IT and Cybersecurity Occupations. Ottawa: Government of Canada. Table 14-10-0031-01 and Table 14-10-0371-01

ApplyBoard. 2024. "The Impacts of Canada's International Student Cap on Postgraduate Studies." ApplyBoard Insights.

BLG (Borden Ladner Gervais LLP). 2024. "Additional updates to Canada's international student program." April 12, 2024.

The Global Race for Cybersecurity and Innovation by François Guay

Demographics and GDP

1. Statistics Canada Population Estimate
2. IMF Datacommons Israel Population
3. Datacommons Singapore Population
4. Global Finance Magazine Estonia Data
5. Wikipedia Canada GDP
6. Wikipedia Israel GDP
7. Wikipedia Singapore GDP

Startup and Innovation Ecosystem Data

8. StartupBlink Canada Startup Count
9. The Recursive Israel Startup Ecosystem
10. UBESG Singapore Startup Data
11. Startup Estonia Data
12. Yahoo Finance Canada Unicorn Count
13. The Recursive Israel Unicorn Count
14. StartupBlink Singapore Unicorn Data

References

15. SBR Singapore Unicorn Data
16. Startup Estonia Unicorn Count
17. CVCA Canada Venture and Exit Data
18. JNS Israel Tech Exits Including Wiz Acquisition
19. Enterprise Singapore Venture and Deal Data
20. Invest in Estonia VC and GDP Metrics
21. Crunchbase Global VC Rankings
22. Dealroom Global VC Rankings

Cybersecurity Readiness and Government Spending

23. Cyber Magazine Global Cybersecurity Index
24. IMD World Digital Competitiveness Ranking
25. Cyber Security Agency of Singapore National Investment
26. World Bank Cyber Spending Data
27. VuMetric Israel Government Cyber Investment


ccn