KPMG

Cyber Incidents and Intelligence: 2025

KPMG Canada's Cyber Incident Response and Cyber Threat Intelligence Year-in-Review

March 2026

2025 Canadian Report

kpmg.ca

Table of Contents

01 Introduction 01

02 Incident Response

Summary 02
IR Incidents 07
Key Learnings: Enhancing Detection and Response Maturity 10
Looking Forward to 2026 12

03 Cyber Threat Intelligence

Introduction 13
State-Backed Adversaries in 2025 15
Artificial Intelligence in 2025: Trends in the Digital Landscape 18
Looking Forward to 2026 19

04 How KPMG can Help 22

05 Contributors 23

06 Contact Us 24

01 Introduction

Cyber threats continue to escalate in scale, sophistication, and reach. In 2025, KPMG Canada's cyber incident response (IR) teams observed organizations across Canada experiencing a surge in cross-border threat activity, rapid exploitation of high-impact vulnerabilities, and increased operational maturity among both financially motivated and state-aligned adversaries.

From a KPMG Canada incident responder's perspective, 2025 has been defined less by a single dominant ransomware cartel and more by high-volume, fast-moving Ransomware as a Service ("RaaS") ecosystems impacting Canadian organizations. Groups such as **Akira, RansomHub, Qilin**, and **PLAY** appear most frequently across live Canadian cases, reflecting a sustained pattern of repeat activity rather than reliance on a single actor. These groups typically leverage compromised credentials, unpatched edge infrastructure, or poorly governed remote access to move quickly to impact.

Rhysida, Medusa, MetaEncrypter, INC Ransom, BlackByte (Crux), Sinobi and emerging or rebranded variants continue to surface intermittently, reinforcing the fluidity of the ecosystem. While legacy or disrupted operations (such as **LockBit** derived activity using leaked builders) still appear, their presence is secondary to the volume driven RaaS model. What stands out operationally is the churn: new names appear, rebrand, or disappear rapidly, but the tradecraft remains consistent: identity abuse, speed over stealth, double-extortion, and pressure on business operations rather than technical persistence.

Canadian organizations are no longer treating cyber insurance as a passive financial backstop; it has become a forcing function for better security hygiene. From what KPMG frontline responders are observing across active breach engagements in Canada, insurers are increasingly shaping minimum standards in real environments. Multi-factor authentication (MFA) gaps, over-privileged identities, misconfigured endpoint detection and response (EDR) deployments, weak logging, and poor patch discipline are still the most common root causes seen in insured incidents.

As a result, organizations are aligning security roadmaps directly to insurer expectations, tightening identity and access management, validating backups and recovery procedures, improving asset visibility, and operationalizing detection rather than assuming tools alone are sufficient. Premiums, coverage limits, and even claim eligibility are now directly tied to whether these controls work in practice, not just whether they exist on paper.

KPMG responders in Canada are also seeing cyber insurance materially influence incident response maturity. Many Canadian organizations now maintain pre-negotiated IR retainers, breach counsel, and crisis communications pathways because insurers expect rapid, disciplined execution in the first 24 to 72 hours of an incident.

In real breaches, the difference between a contained event and a business-wide crisis often comes down to preparedness: clear decision rights, tested playbooks, and the ability to produce defensible forensic evidence quickly. Post-incident, insurers increasingly scrutinize root cause and control failures, which feeds directly back into security investment decisions. The net effect is that cyber insurance is becoming embedded in enterprise risk governance not just to pay for breaches, but to actively reduce their likelihood, scope, and impact.

This report offers a Canadian perspective on the cyber incidents investigated by KPMG in Canada, highlighting major trends, threat actor behaviours, and industry-specific insights observed throughout 2025. Developed collaboratively by KPMG Canada's Cyber Incident Response and Cyber Threat Intelligence teams, the report provides data-driven analysis, strategic lessons learned, and forward-looking considerations to help Canadian organizations enhance their security posture.

Findings are derived from real incidents handled by KPMG Canada's cyber incident responders in 2025. While the nature of these events is accurately reflected, identifying information has been removed to preserve confidentiality.

02 Incident Response

Summary

Overview of Incident Trends

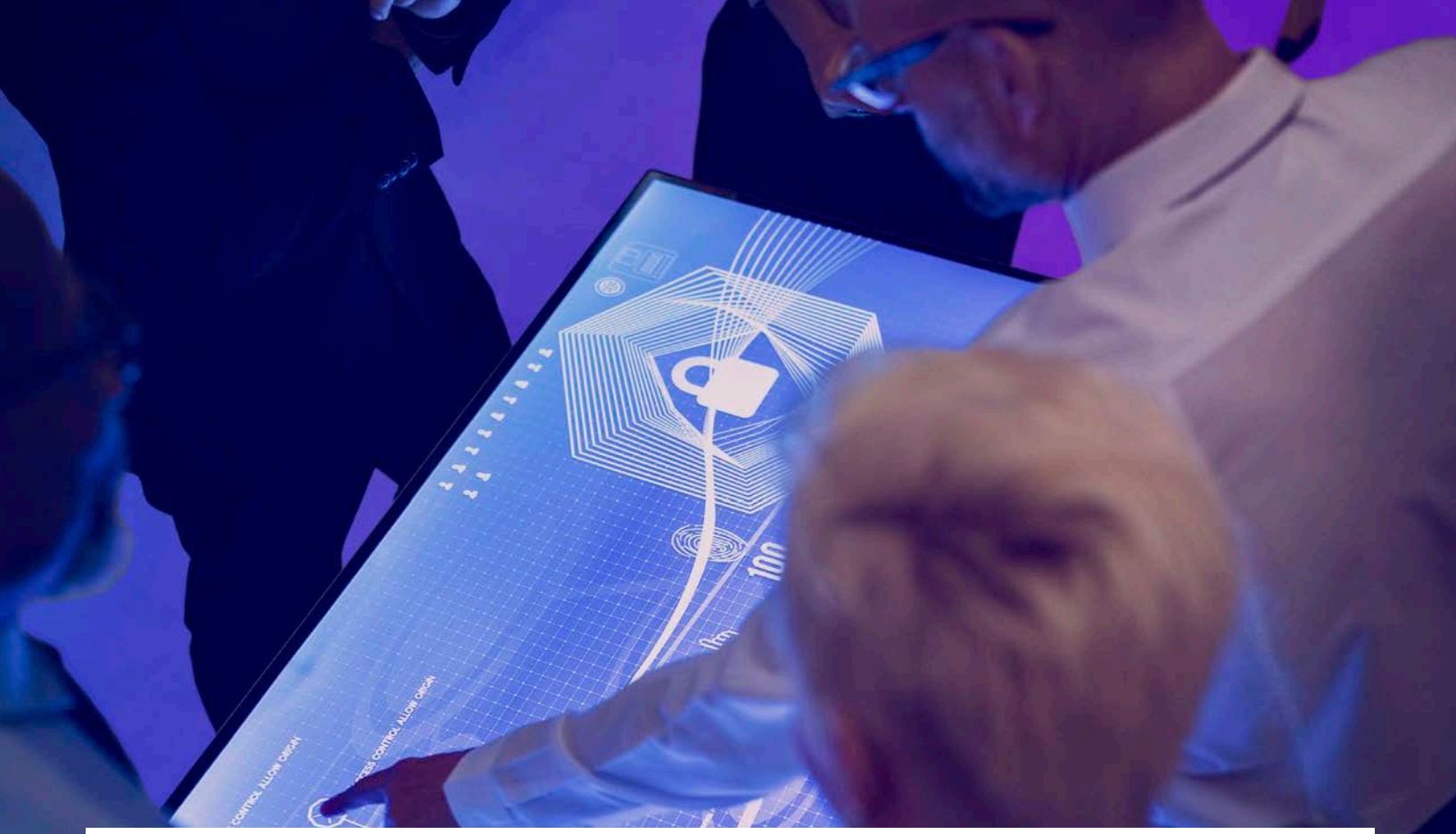
In 2025, KPMG Canada responded to **120+ cyber incidents** across a broad cross-section of Canadian organizations, reflecting both the sustained threat environment and continued demand for rapid, coordinated incident response support. These engagements ranged from ransomware and data extortion events to business email compromise (BEC), insider driven incidents, and intrusions originating from third-party or supply chain exposures. While the nature and scale of incidents varied, the overall volume underscores that cyber incidents are no longer exceptional events, but a persistent operational risk facing organizations across sectors.

The incident volume observed in 2025 highlights two consistent themes:

01 First, threat activity remains opportunistic and scalable, with attackers prioritizing speed, access, and business impact over long-term persistence.

02 Second, organizational exposure is increasingly shaped by a small number of recurring control failures.

Most common failures are identity and access weaknesses, incomplete visibility across hybrid environments, and delayed detection of initial compromise. In many cases, incidents escalated rapidly because foundational controls failed to operate as intended.



From an operational perspective, the 120+ incidents responded to in 2025 reinforce the importance of readiness. Organizations with pre-established incident response retainers, clearly defined escalation pathways, and tested response playbooks achieved faster containment and reduced business disruption. Conversely, organizations engaging response services reactively often faced longer dwell times, broader impact, and greater uncertainty in the critical early stages of an incident.

Taken together, the 2025 incident landscape in Canada reflects a threat environment defined by volume, repeatable attack patterns, and increasing pressure on organizations to demonstrate not just the presence of controls, but their effectiveness under real-world conditions.

Artificial Intelligence (AI) Adoption and Its Dual Role in Incident Activity

While truly autonomous AI driven malware has not yet been observed in the wild, 2025 marked a notable rise in threat actors using large language models (LLMs), such as ChatGPT, Gemini, and other publicly available tools, to enhance their operations during active breaches.

Threat actors increasingly rely on AI to troubleshoot exploitation errors, refine attack paths, and adjust tactics at run time, similar to how early career developers use LLMs to solve technical challenges. In several investigations this year, AI was also used by adversaries to draft extortion communications and improve negotiation strategies, resulting in more polished and targeted interactions with victims.

At the same time, incident responders are harnessing AI to accelerate forensic and analytical activities, which has reshaped response timelines. Tasks that previously required manual reverse engineering, such as obfuscating scripts, interpreting encoded payloads, or identifying malicious logic embedded in offensive tools, can now be completed within seconds using AI assisted analysis.

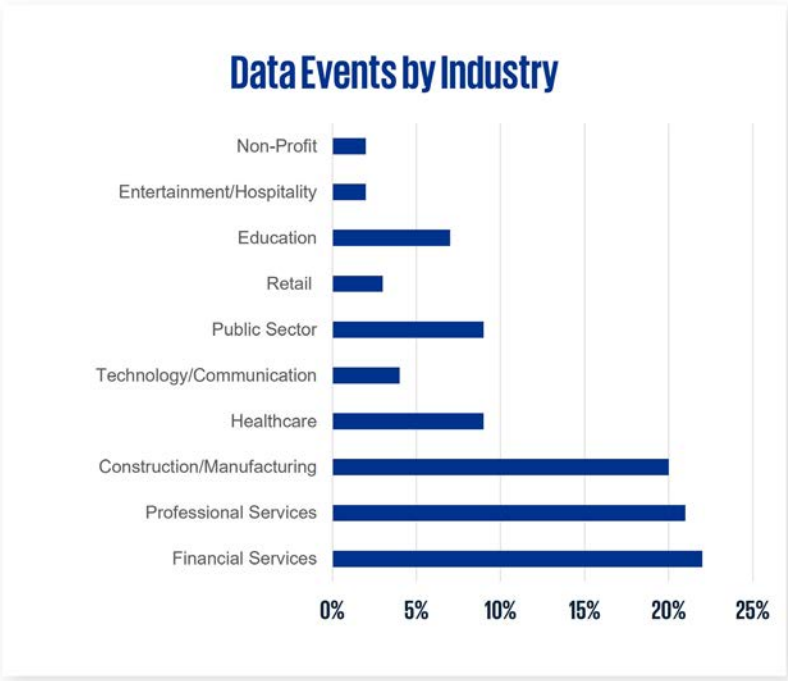
These capabilities reduce investigative cycle times, improve accuracy, and allow responders to redirect their effort toward higher value activities such as adversary attribution, containment strategy, and risk quantification. The growing integration of AI across both threat activity and defensive operations reflects a significant shift in how incidents unfold and how organizations prepare for response.

Major Threats and Statistics

2025 Events by Industry

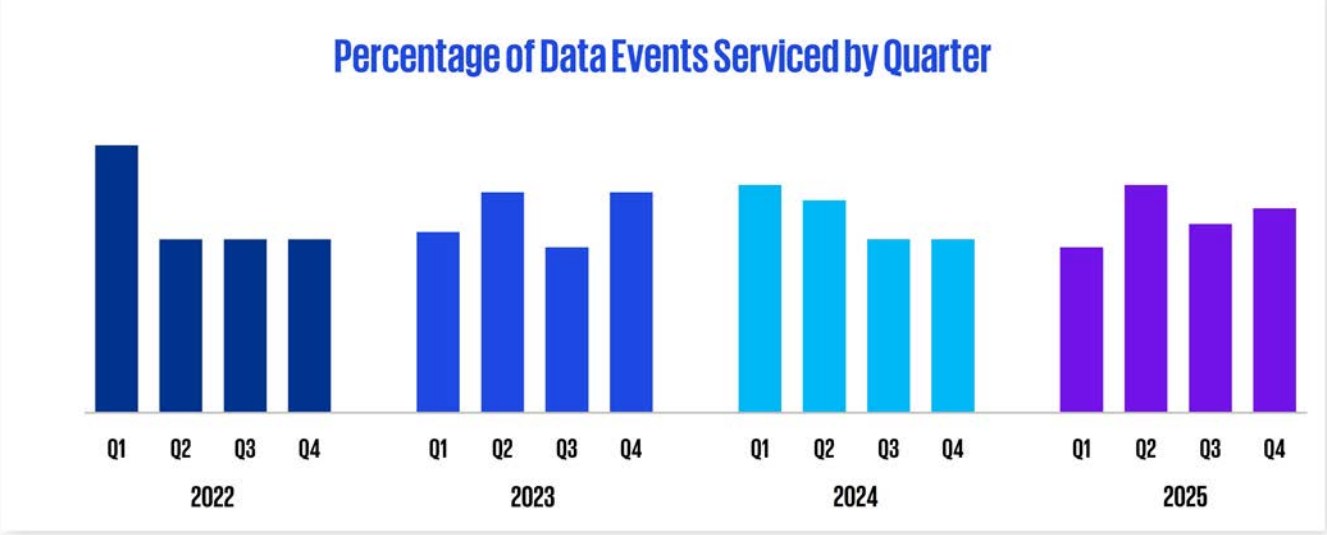
In 2025, Canadian organizations continued to operate in a challenging cyber risk environment, where evolving attack techniques, persistent data exposure, and downstream identity impacts increased pressure to strengthen cybersecurity and privacy practices. Cyber incidents and identity-related risk remain closely linked, as data events frequently enable identity theft and fraud well beyond the initial compromise. To provide additional context on these trends, TransUnion presents insights based on its analysis of data events and identity protection activity within the Canadian threat landscape.

TransUnion, a credit reporting agency offering monitoring services in Canada, the United States, the United Kingdom, India, Hong Kong (SAR), China, and South Africa, shared insights into trends observed within the Canadian threat landscape and the resulting impacts on identity theft.



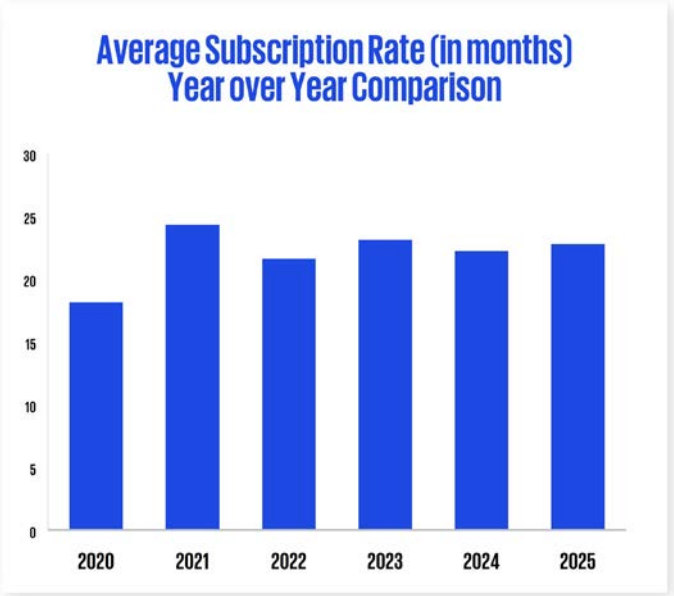
Source: TransUnion Canada Breach & Cyber Risk Solutions records

Data shared by TransUnion indicates that data events in 2025 were most concentrated in financial services, professional services, and construction/manufacturing, reflecting the continued targeting of data rich and operationally dependent sectors.



Source: TransUnion Canada Breach & Cyber Risk Solutions records

Quarterly distribution of data events remained relatively consistent over time, suggesting a steady baseline of incident activity rather than pronounced seasonal spikes. Average identity monitoring subscription lengths have remained stable at approximately one to two years, indicating sustained identity risk following data events rather than short-term exposure.



Source: TransUnion Canada Breach & Cyber Risk Solutions records

Incident Classification Metrics

In 2025, the majority of incidents responded to by KPMG Canada fell into a small number of recurring incident classes, reflecting both attacker preference and systemic organizational exposure.

Ransomware remained the dominant incident type, accounting for nearly half of all response engagements, followed closely by business email compromise (BEC). Together, these financially motivated attack types represented the vast majority of incidents, underscoring the continued focus on rapid monetization and business disruption.

Intrusion-based incidents, including unauthorized access and malware-driven activity not immediately tied to ransomware, comprised a smaller but consistent portion of engagements. Insider-related incidents and other event types, such as standalone data breaches or data exfiltration without encryption, occurred less frequently.

While tactics may vary, attackers continue to prioritize speed, access to identities, and pathways to financial or operational impact over prolonged persistence.

Incident Type	% of Incidents
Ransomware	49.20%
Business Email Compromise (BEC)	35.80%
Intrusion	10.80%
Other (Data Breach, Data Exfiltration, Other)	2.50%
Insider Threat	1.70%

Early Threat Actor Engagement: Insights From RedInc on Timing, Control, and Communication

According to RedInc, a Canadian based threat actor engagement service, breach events may begin with technical compromise, but the outcome is driven by human factors—especially how and when communication with the threat actor occurs. Their analysis indicates that early engagement provides the strongest foundation for control. It enables stronger verification of claims, assessment of actual exposure , and the ability to shape negotiation tone before demands escalate or threats of data release surface.

RedInc reports that threat actors consistently impose compressed timelines intended to induce urgency. However, based on their case data, initial deadlines have been extended in every engagement to date, with negotiation periods averaging approximately 21 days. RedInc notes that the shortest extension observed was 3 days, while the longest was 24 days, with an average extension of 9.8 days across cases. Extensions result not from confrontation, but from strategic communication that identifies when pressure can be paused.

Gaining time early meaningfully shifts leverage. With reduced pressure, organizations can evaluate restoration options, coordinate internal stakeholders, and negotiate from a more informed position. RedInc's aggregated outcomes show that extended timelines strongly correlate with materially lower financial exposure, with average ransom reductions of 62%, and typical results ranging from 50% to 75% for their cases.

RedInc underscores that communication discipline is central to these outcomes. Because threat actor messages may later become public or subject to legal scrutiny, tone, pacing, and consistency must be intentional. When communication is treated as a strategic function—not a reactive exchange—it becomes a tool for stability, enabling decisions that minimize loss, preserve governance processes, and protect organizational integrity.

Overall, the objective of threat actor engagement remains consistent: to reduce loss severity, protect reputational integrity, and support legally defensible outcomes for organizations.

Powered by former law enforcement hostage negotiators and cybercrime investigators, RedInc. specializes in managing highpressure ransomware communications. By combining deep psychological insight with technical intelligence, they safely engage threat actors, coordinate complex payment processes when required, and secure the decryption and release of compromised data. This integrated approach makes RedInc. a trusted partner for organizations navigating the risks and complexities of ransomware incidents.

IR Incidents

Key Investigation Case Studies

Case Study #1 - Education Sector - Insider Threat Case Study

Overview

An organization in the education sector identified an internally driven security incident after deploying a new EDR solution that detected malware on an employee workstation. Investigation revealed that the employee had intentionally executed offensive security tools, attempted credential theft, and conducted unauthorized security testing across the corporate environment. The user held a standard account but expanded their access through misuse of credential harvesting utilities and reconnaissance activity.

This case highlights how insider misuse - whether curiosity driven or malicious - can result in significant exposure when monitoring controls, privilege management, and behavioural analytics are not fully mature. Early detection through EDR deployment prevented the incident from escalating further and underscored the need for continuous visibility into privileged activity.

Threat Actor Profile

Attribution:	Known insider (employee)
Motivation:	Unauthorized security experimentation, privilege escalation, and attempted credential compromise
Access Level:	Standard employee account with access expanded through misuse of offensive tools
Behaviours:	Persistent credential harvesting, reconnaissance, unauthorized data aggregation, removable-media exfiltration

Threat Actor Activity (TTPs Observed)

Initial Access

- Employee with access into the IT environment
- Executed offensive security tools undetected prior to EDR alerts
- Insufficient restrictions around PowerShell, credential stores, and removable media
- Capability to access sensitive directories and authentication systems (active Directory, KeePass stores, ERP references)

Reconnaissance

- Internal network scan results
- System information exports
- Tools and scripts used to probe and test internal systems

Privilege Escalation

- Mimikatz for credential extraction
- PowerSploit for exploitation and post-exploitation activity
- Impacket modules for lateral movement and credential operations

Exfiltration

Removable media used for exfilteration:

- KeePass password database files
- ERP-related references
- Files names suggesting organized data staging
- Credential sets and other sensitive exports copied to USB

Case Study #2 – MetaEncryptor

An organization in the legal sector was hit by a MetaEncrypter (also known as MetaEncryptor), lesser-known ransomware group which uses the MetaPowder ransomware, that has been active since at least 2023. The incident came the light when ransom notes and encrypted files were discovered in the morning, following the encryption of the environment overnight. In this incident, the threat actor managed to stay under the radar for close to a month, from initial access to impact (encryption). During that time, they moved from a single compromised user workstation, compromising a legacy account which was part of the Domain Admins group, and moved laterally to two (2) servers, holding their position in the network. Most of their attack was then orchestrated from these systems, by leveraging built-in Windows tools and protocols such as PowerShell, PowerShell Remoting, WinRM, WMI and Scheduled Tasks to execute their attack. They identified servers of interest to exfiltrate data from and once complete, proceeded with the encryption.

This case highlights how some threat actors will stick to their tactics, techniques and procedures, alongside tools if these prove to be effective and work. For MetaEncrypter, the various indicators of compromises, indicators of attacks and TTPs observed in that incident are the same as the ones that were observed back in 2023, down to the initial access method that was used and the folder names used to host their tools, output files, scripts, etc.

Threat Actor Profile

Attribution:	MetaEncrypter/MetaEncryptor
Motivation:	Financial (extortion)
Access Level:	Standard user account on a domain-joined PC that was then used for identity attacks against Active Directory

Threat Actor Activity (TTPs Observed)

InitialAccess:	Compromised user workstation via NetSupport RAT
Execution:	PsExec
Credential Access:	Identity-based attacks against Active Directory (e.g.: Kerberoasting)
Lateral Movement & Execution:	Built-in Windows tools and protocols (PowerShell, PowerShell Remoting, WinRM, WMI and Scheduled Tasks)
Collection:	WinRAR via the command-line
Exfiltration:	Exfiltration to a Cloud service using an open-source client (megacmd) Impact: Local encryption of physical servers, and encryption of virtualization hosts (Hyper-V)
Impact:	Local encryption of physical servers, and encryption of virtualization hosts (Hyper-V)

Key Negotiation Case Studies

Case Study 1: When Uncontrolled Communication Becomes Leverage

An organization impacted by a Qilinecosystem ransomware affiliate experienced early complications when an internal employee began communicating directly with the threat actor. Lacking training or negotiation awareness, the employee shared sensitive operational and financial information, failed to validate extortion claims, and made an uninformed initial offer. The threat actor used these disclosures to justify a hardened negotiation stance.

After communication ceased, the employee continued accessing the chat portal—activity monitored by the attacker—resulting in 15 days of perceived organizational silence.

When professional support was engaged, negotiations were restarted, claims revalidated, and communication cadence reset. Over 29 additional days, the organization restored systems independently and ultimately resolved the incident without relying on the attacker.

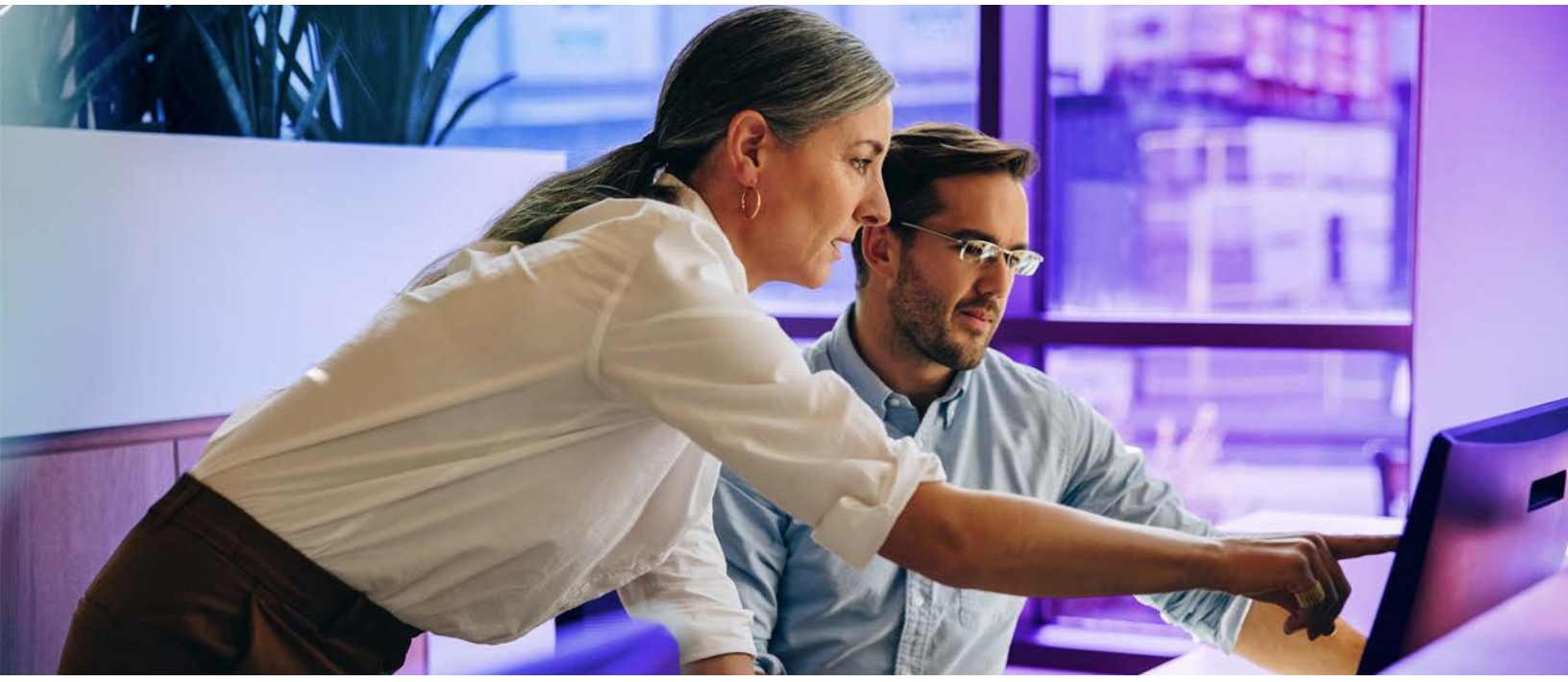
This case demonstrates how unmanaged communication can unintentionally strengthen a threat actor's position, while disciplined engagement can reestablish control even after early missteps.

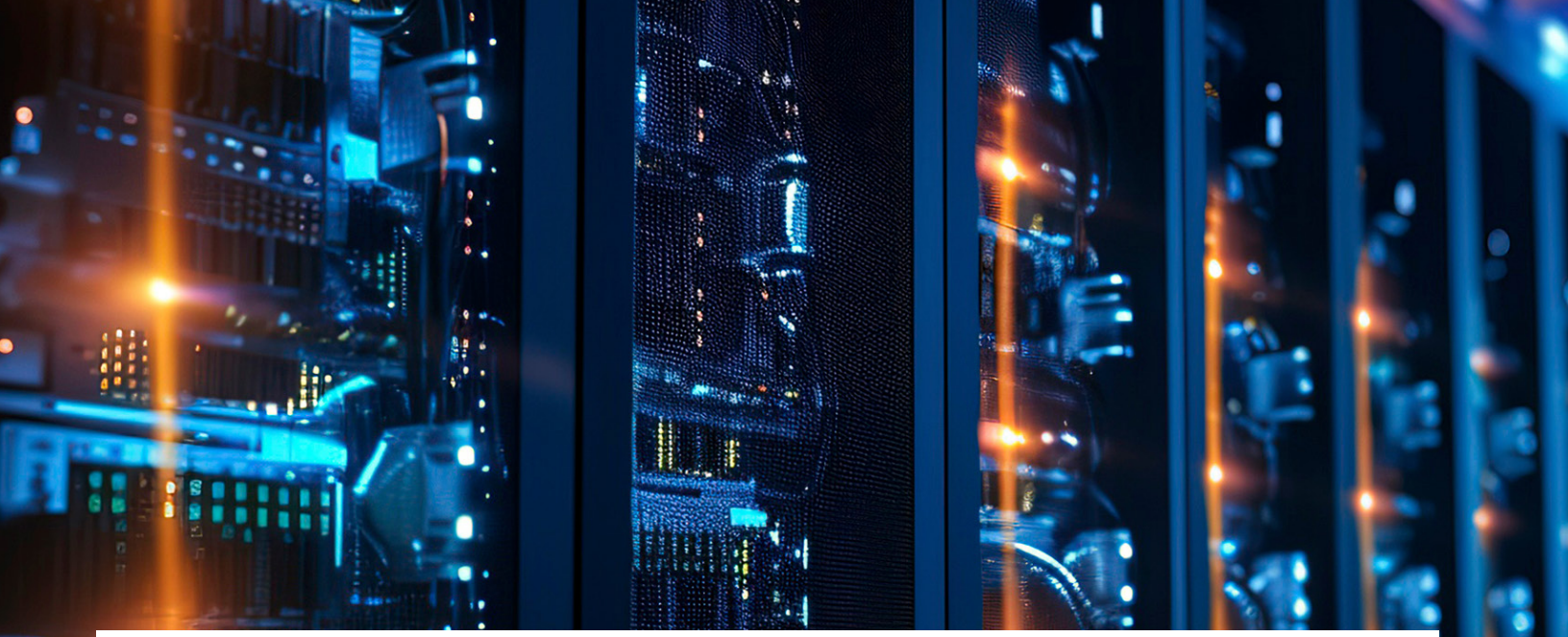
Case Study 2: Early Engagement Validated No Data Exfiltration

An organization targeted by an Akiraecosystem ransomware affiliate received a ransom note alleging data theft, encryption, and threats of sale on the dark web. Early engagement with the threat actor quickly revealed that the claims of exfiltration were generic and not specific to the client. No data theft had occurred; only encryption was confirmed.

Because the client maintained reliable backups, systems were restored without reliance on the attacker. Over a 15day negotiation period, the ransom demand was reduced by 60%, and the organization made an informed decision not to proceed with payment.

This case illustrates how early communication can validate or disprove threat actor claims, enabling evidence based decision making and preventing unnecessary financial loss.





Key Learnings: Enhancing Detection and Response Maturity

In 2025, incident response engagements in Canada continued to demonstrate that systemic weaknesses in identity controls, credential management, patching practices, and user awareness remain central drivers of successful compromise. These gaps are frequently compounded by limited detection and response capabilities, which allow threat actors to progress from initial access to material impact before containment measures are initiated. As attack paths become increasingly automated and opportunistic, traditional control implementations alone are often insufficient to meaningfully reduce disruption or dwell time.

For CISOs and IT leaders across Canadian organizations, these observations reinforce the importance of investing in advanced detection and response capabilities that enhance organizational resilience and enable faster, more effective containment. Solutions that leverage AI-driven analytics and agentic response workflows can help prioritize high-risk activity, support rapid investigation and containment actions, and reduce the operational burden on internal teams during incidents. Managed Detection and Response services that incorporate these capabilities provide organizations with an opportunity to improve response consistency, accelerate decision-making, and limit business disruption resulting from both financially motivated and state-aligned threat activity.

KPMG Canada's incident responders have identified five focus areas that reflect the industry's shift from reactive to predictive and adaptive security, aligned with the reality that attackers are increasingly leveraging automation and AI—making speed and intelligence the new differentiators in defence.

1. Strengthening Identity Controls: The Centre Stage of Cybersecurity

Leading Canadian organizations recognize that identity now serves as the new perimeter in cybersecurity. To address this shift, organizations are implementing Identity Threat Detection and Response (ITDR) capabilities, deploying robust Privileged Access Management (PAM) frameworks, and adopting Just-In-Time (JIT) access models.

These initiatives are designed to enforce least-privilege principles and enable continuous monitoring of identity behaviours for signs of anomalous activity. In response to hybrid work models and expanded cloud adoption, organizations are prioritizing comprehensive identity governance strategies to reduce the risk of lateral movement and privilege escalation.

In parallel, organizations are reinforcing Multi-Factor Authentication (MFA) across critical systems, supported by strengthened password policies and enterprise-grade password management tools. These technical controls are complemented by ongoing user awareness initiatives, including targeted phishing simulations and training campaigns, to help employees recognize and respond to social engineering attempts. This continued focus on human-centric defence remains essential to mitigating credential-based attacks and maintaining operational resilience.

2. Cyber Resilience and Cyber Resilience and Backups

Canadian organizations are elevating their backup strategies to address modern threats such as ransomware and destructive cyberattacks. Recognizing that backups are foundational to cyber resilience, organizations are deploying immutable and air-gapped solutions designed to prevent unauthorized modification or access by threat actors. These architectures are distributed across on-premises and cloud environments to improve redundancy and recovery capability.

To further strengthen resilience, organizations are automating backup processes to ensure recovery points remain current and reliable. Regular restore testing is increasingly treated as a standard practice and integrated into incident response planning. This ensures that backup systems are not only present, but operationally effective when required, enabling faster recovery and minimizing business disruption during incidents.

3. Drive Towards Agentic Platforms and AI-Based Enablers

ISOs and IT leaders in Canada are increasingly focused on learning, evaluating, and adopting AI-driven security platforms that operate as agentic systems—autonomous, adaptive, and capable of orchestrating coordinated responses across endpoints, networks, and cloud environments. These platforms leverage machine learning to identify anomalous activity, apply predictive analytics to anticipate emerging threats, and execute automated response playbooks to support rapid containment.

Looking ahead, AI-enabled capabilities are expected to become a primary driver of security investment. By adopting these technologies, organizations are positioning themselves to defend against automated and AI-assisted attacks while scaling security operations without proportional increases in staffing. This reflects a broader shift toward intelligence-driven, resilient defence models aligned to the realities of the current threat landscape.

4. Proactive Defence: MSS, Threat Hunting, Purple Teaming, Red Teaming, and CTI

Leading Canadian organizations are increasingly moving beyond reactive security models and adopting proactive defence strategies. Investments in Managed Security Services (MSS) enable continuous, 24/7 monitoring, often enhanced through AI-based analytics, supporting earlier detection and faster response to emerging threats.

Threat hunting programs are being used to proactively identify stealthy adversaries and techniques that evade traditional controls. Purple Teaming initiatives—integrating offensive and defensive capabilities—are being conducted more regularly to validate detection coverage and improve response effectiveness. Cyber Threat Intelligence (CTI) has become a core input into security decision-making, enabling organizations to prioritize controls and investments based on real-world adversary behaviour. Together, these activities reduce attacker dwell time and strengthen organizational resilience.

5. Prepare for the Worst: IR Readiness and Tabletop Exercises

Incident response readiness has become a baseline operational requirement for Canadian organizations. CISOs and IT leaders are increasingly conducting tabletop exercises and simulated ransomware scenarios to test decision-making, business continuity, and disaster recovery capabilities under realistic conditions. Many organizations have established pre-negotiated arrangements with forensic, legal, and communications partners to ensure rapid mobilization during an incident.

By embedding IR readiness into standard operating practices, organizations are reducing uncertainty, limiting operational disruption, and improving regulatory defensibility. These measures position organizations to respond decisively and effectively when—rather than if—a significant cyber incident occurs.

Looking Forward to 2026

Outlook, Strategy, Challenges

Looking ahead, 2026 is likely to be a year of continued flux in the cyber threat landscape facing Canadian organizations. While established threats such as ransomware and hacktivism are expected to persist, the introduction and maturation of new technologies is likely to have a greater impact than observed in 2025.

As the initial hype surrounding artificial intelligence begins to subside, the practical realities of what AI can and cannot deliver in a defensive context are becoming clearer. At the same time, the ability for threat actors to leverage AI to enhance social engineering, phishing, and impersonation campaigns is accelerating. While concerns around autonomous or AI-enabled ransomware remain, the more immediate and material risk is likely to stem from increasingly convincing social engineering attacks that exploit the human vulnerabilities present in every organization.

In parallel, the global geopolitical environment is expected to remain volatile, with potential implications for Canada's cyber threat landscape. Heightened geopolitical tensions may drive increased levels of state-sponsored cyber espionage and the pre-positioning of access within critical infrastructure environments. As tensions rise, cyber activity designed to disrupt or degrade energy, communications, and other critical technologies may increase, potentially alongside information operations that leverage cyber capabilities to influence public perception. These dynamics may also contribute to greater efforts by both criminal and state-aligned actors to recruit or coerce insiders, increasing the risk of insider-enabled attacks as part of broader cyber campaigns.

03 Cyber Threat Intelligence

Introduction

2025 was a year of change and increased uncertainty. Through elections, geopolitical actions, economic policies and cultural shifts, the overall threat landscape evolved in a fundamental way.

While changes have impacted trade negotiations and physical security around the globe, it is also having an increasing impact on the view of Cyber. Previous assumptions about the roles of state-backed APTs (advanced persistent threats), cyber crime and the threat landscape can no longer be counted on, organizations must start to consider their position in the national order and how they may be targeted to effectuate a geopolitical goal.

At the same time as this shift, cyber threats against critical infrastructure, government institutions, and commercial platforms intensified in scale, sophistication, and impact. State-aligned actors across regimes demonstrated sustained focus on energy, telecommunications, transportation, and industrial systems, often exploiting misconfigurations, trusted relationships, and supply-chain dependencies rather than novel vulnerabilities alone. These campaigns blurred traditional distinctions between espionage, disruption, and cybercrime, with ransomware, extortion, and public-facing attacks increasingly overlapping with nation-state objectives. The result has been heightened operational risk for both public and private organizations.

Emerging technologies further reshaped the threat landscape. Artificial intelligence accelerated both defensive and offensive cyber capabilities, introducing new efficiencies while creating novel vulnerabilities and governance challenges. In parallel, high-profile breaches involving major cloud and enterprise software providers underscored the systemic risks posed by third-party integrations and identity-centric attacks. Together, these developments highlight a cybersecurity environment defined less by isolated incidents and more by persistent, strategic pressure where digital resilience, supply-chain security, and policy alignment have become critical determinants of national and organizational security. determinants of national and organizational security.

Geopolitics in Cyberspace: Alliances, Laws, and National Security Decisions

China Expanding Cooperation in Cybersecurity with Russia

China announced an expansion of its cybersecurity cooperation with Russia in early 2025. The Chinese Ambassador to Russia emphasized Beijing's intention to deepen collaboration not only with Russia but also with countries worldwide, aiming to create a shared future in cyberspace. In an April 2025 statement, the Ambassador asserted that China is committed to establishing what he described as a "multilateral, democratic, and transparent global internet governance system." He stressed that cyberspace should not serve as a battleground for a global power rivalry but should instead be a platform for international cooperation. In the same article addressing these developments, the Chinese ambassador suggested the United States had targeted Russia's critical infrastructure through malicious cyberattacks. However, some analysts argue that this strengthening of cybersecurity ties between China and Russia signals a broader inclination among non-Western powers to influence the rules and norms governing the Internet, especially considering the ongoing geopolitical tensions with the United States and its allies.

Proposed Russian Law on Vulnerability Reporting

Russia is preparing to vote on legislation that would require all software vulnerabilities discovered within its borders to be reported to the government before disclosure to vendors or other parties. The bill, under consideration since 2022 and reportedly slated for a decision soon, would establish a unified reporting system across multiple Russian agencies. It would mandate the registration of security researchers and companies that run bug bounty programs, require researchers to disclose their real identities to authorities, and impose criminal penalties for non-compliance. This approach closely mirrors China's 2021 regulations on vulnerability disclosure, which expanded state control over vulnerability intelligence.

If enacted, the law would significantly increase the Russian government's access to undisclosed (zero-day) vulnerabilities, creating opportunities for state-sponsored groups to accelerate espionage and, over time, potentially conduct more disruptive cyber operations.

Specifically, the proposal would create official registries for companies operating bug bounty programs and for security researchers. Researchers would be required to disclose their real identities to Russian authorities. The bill would criminalize failing to report discovered vulnerabilities, exposing non-reporting researchers to potential prosecution.

For Western organizations operating in Russia, these reporting requirements would introduce strategic risks by compelling the sharing of sensitive technical information with state agencies, raising concerns about espionage and coercion. While immediate operational impacts may be limited, the longer-term effect could be a more aggressive and capable Russian cyber threat landscape, broadly paralleling developments observed in China after the introduction of comparable rules.

Canada Bans Hikvision Over Security Concerns

Hikvision, one of the world's largest surveillance camera manufacturers, has operated in Canada since 2014. However, its extensive global presence and ties to state-backed projects in China have sparked concerns among Western countries and are believed to play a pivotal role in the Canadian government's decision to ban the camera in the country. These developments have led to parallels with previous crackdowns on Huawei, where classified intelligence justified sweeping commercial restrictions. The United States, the United Kingdom, and Australia have already adopted measures against Hikvision, citing allegations that its cameras were utilized to monitor Uyghur people in Xinjiang—a claim that Beijing adamantly denies. Additionally, the FBI has issued warnings concerning webcam malware and the broader cybersecurity hazards associated with Chinese IoT devices,. Reports bolster these concerns, such as a 2023 investigation revealing over 40,000 unprotected security cameras, some of them Hikvision devices, freely streaming live footage from private homes, offices, and sensitive infrastructure. Such vulnerabilities expose individuals and organizations to surveillance, industrial espionage, and privacy breaches.

State-Backed Adversaries in 2025

Inside Sandworm's Evolving Infrastructure Attacks

Russian government–aligned threat actors were observed conducting attacks against misconfigured network edge devices, resulting in the compromise of more than ten organizations. These activities have been attributed to the well-known nation-state threat group Sandworm, also tracked as APT44 or Seashell Blizzard, which U.S. authorities have linked to Russia's Main Intelligence Directorate (GRU).

This campaign was initially monitored by researchers in 2021, when it was determined that the campaign was targeting Western critical infrastructure, with a particular focus on the energy sector. Researchers were able to identify malicious activity involving customer-owned network edge devices within a popular cloud environment. The operator of that cloud environment stated that incidents were not a result of vulnerabilities in their service, but stemmed from misconfiguration in customer-managed devices.

Threat actors compromised customer network edge devices hosted in the cloud, intercepting network traffic to harvest credentials, then leveraged those credentials to access additional services and infrastructure. Threat actors subsequently established persistent access, enabling lateral movement within the environment. Historically, Sandworm has relied on exploiting software vulnerabilities to gain initial access. However, this campaign marked a notable shift in tactics, as the group increasingly leveraged misconfigurations and credential interception. While the group's strategic objectives remained consistent, this approach would likely reduce operational exposure and detection risk.

Researchers reported that in 2025, the adversaries successfully accessed endpoints across multiple sectors, including electric utilities, energy providers, and managed security service providers that support energy-sector clients. The campaign also expanded to include telecommunications providers and technology companies.

Sandworm has long been associated with attacks targeting critical infrastructure and energy organizations worldwide, particularly in Ukraine. The evolution observed during the 2025 campaign underscores the group's continued adaptation and sustained focus on high-impact strategic targets.

Canadian Industrial Control Systems (ICS) Victimized by Threat Actors

In late October 2025, the Cyber Centre and the Royal Canadian Mounted Police warned of multiple reports of incidents involving internet-accessible ICS. Impacted organizations included a water facility that had its water pressure values tampered with, resulting in degraded service for its community; a Canadian oil and gas company, where an Automated Tank Gauge (ATG) was manipulated, triggering false alarms; and a Canadian farm that had suffered manipulation of its temperature and humidity levels in its grain drying silo.

The Canadian authorities alert did not attribute the incidents to a specific group; however, similar threat groups linked to the Russian government-aligned groups attacked the industrial control systems of multiple U.S. and European critical infrastructure organizations.

Canada's cyber agency warned that many smaller utilities, farms, and manufacturers continue to run poorly secured internet-connected systems, leaving them vulnerable to opportunistic attacks.

Iranian state-sponsored APT

On September 17, 2025, researchers reported that the Iranian state-sponsored APT group, Subtle Snail, compromised 34 devices across eleven organizations during a week-long campaign targeting European telecommunications firms, while also maintaining an interest in the aerospace and defence sectors. The affected companies were located in Canada, France, the United Arab Emirates, the United Kingdom, and the United States.

Subtle Snail has been linked to the Islamic Revolutionary Guard Corps (IRGC)—conducted the campaign by posing as HR personnel on LinkedIn and directing victims to fraudulent application or interview-scheduling pages that delivered malicious archive files.

Chinese state-backed Group Salt Typhoon: Targeted More than 80 Countries, 600 Companies

In 2025, cyber authorities from thirteen countries issued a joint cybersecurity advisory warning that threat activity partially overlapped with activity tracked as Salt Typhoon had targeted a wide range of critical infrastructure and industries. Salt Typhoon's operations are not limited to the United States or the telecommunications sector, despite that sector receiving the most public attention. Salt Typhoon activity has affected more than 80 countries and over 600 companies worldwide.

In June 2025, the FBI and the Canadian Centre for Cyber Security reported that Salt Typhoon had targeted a Canadian telecommunications provider, exploiting vulnerabilities in network infrastructure to gain access.

In July 2025, further disclosures indicated that Salt Typhoon activity had also targeted U.S. Army National Guard networks between March and December 2024.

An August 2025 joint advisory—along with additional notices from agencies such as the United Kingdom's National Cyber Security Centre—revealed that Salt Typhoon had almost certainly targeted organizations in the United States, Australia, Canada, New Zealand, the United Kingdom, the Czech Republic, Finland, Germany, Italy, Japan, the Netherlands, Poland, and Spain.

Across these regions, Salt Typhoon's targets have included telecommunications, government, transportation, lodging, and military infrastructure networks. The objective of several intrusions was to maintain persistent, long-term access to victim environments, enabling extensive reconnaissance, data exfiltration, and preparatory access for potential future operations.

Website Defacement

Website defacement represents a significant cybersecurity threat to various sectors, including critical infrastructure organizations. In recent years, there has been a notable increase in incidents involving the defacement of websites. In some instances, the defacement was used to showcase a breach, alerting consumers in real-time about a cyber event. Many organizations globally are targeted by threat actors who deface websites. As the threat landscape evolves, this method may be used to pressure organizations into paying ransoms or addressing the demands of threat actors.

Website Defacement Used to Expose Data Online

More than one million university students attending an institution in New York allegedly had their personal information exposed after a threat actor took over the university's website in March 2025. The attacker reportedly replaced the university homepage with charts and links to large student datasets that categorized standardized test scores by race. The threat actor leaked the personal information of more than three million people, including full names, addresses, phone numbers, grade point averages, email addresses, citizenship status, test scores, majors, ZIP codes, and financial aid information dating back to at least 1989. The attacker is said to be part of a larger group that previously targeted the University of Minnesota and leaked seven million Social Security numbers and other information relating to current and former students. The threat actor claims these attacks are a response to the U.S. Supreme Court's 2023 decision striking down affirmative action in college admissions.

Throughout 2025, KPMG has observed government, energy, education, and other organizations fall victim to website defacements. However, posting large volumes of leaked data for public viewing is less common. With threat groups seeking to increase pressure on organizations to pay ransoms, this tactic could pose a broader risk to targeted entities following a breach.

Canadian Airports Disrupted Following Defacement

In October 2025, Kelowna International Airport, Windsor International Airport in Ontario, Victoria International Airport in British Columbia, and Harrisburg International Airport in Pennsylvania experienced a cyber incident that disrupted terminal information screens and public address systems. A group calling itself "Siberislam" claimed responsibility and shared videos of the attacks online. Kelowna International Airport stated the breach was limited to a cloud-based third-party software provider, with other airport systems remaining secure and isolated. The defaced messages were removed, and affected systems were restored later that day, though some flights were delayed.

Artificial Intelligence in 2025: Trends in the Digital Landscape

DeepSeek Sends Data to Tik Tok Parent Company ByteDance Servers

The DeepSeek iOS app, released on January 25, 2025, was later found to pose significant threats to user data privacy due to its insecure data storage and transmission policies. The app transmits sensitive user information to ByteDance servers without encryption, making it susceptible to interception through Man-in-the-Middle (MITM) attacks. It employs outdated Triple DES (3DES) encryption with hardcoded and reused keys, violating essential cryptographic standards. Additionally, sensitive credentials, including usernames and passwords, are stored insecurely, increasing the risk of theft if devices are compromised. The app collects extensive user and device data, including unique identifiers, which can facilitate detailed tracking and de-anonymization. The routing of user data to ByteDance-controlled servers, under Chinese jurisdiction, raises serious concerns regarding compliance with PRC laws and the potential for government access to this data. The direct transmission of user data to ByteDance's Volcengine cloud service, coupled with the company's ties to the Chinese government and its obligations under PRC surveillance laws, has intensified fears of state-driven data access and surveillance. Despite ByteDance's denials of sharing data with the Chinese government, regulatory agencies and governments remain cautious, leading to immediate bans on the app by several entities to protect national security.

KawaiiGPT: An Open-Source Tool Designed to Bypass AI Safety Controls

A new open-source tool called KawaiiGPT has been released on GitHub. KawaiiGPT is free and functions as an intermediary for AI "jailbreaking." The software connects to existing AI models and delivers their responses to the user. It achieves "unrestricted" outputs by using prompt injection techniques. Standard AI models include safety guardrails to prevent the generation of harmful content. KawaiiGPT can circumvent these protections by embedding a hidden "jailbreak" script that instructs the AI to ignore its safety guidelines. The code for KawaiiGPT is obfuscated, raising concerns among security analysts about whether the software might contain malware.

Shannon: Autonomous AI Pentesting

Shannon is a fully autonomous AI penetration tester that actively discovers and executes real exploits in web applications. Unlike traditional scanners that produce false positives, Shannon delivers proof-of-concept attacks—such as injection exploits, authentication bypass, and SSRF—to confirm actual risk. It closes the gap between continuous code shipping and infrequent pen tests by acting as an on-demand whitebox pentester. With a single command, Shannon performs comprehensive analysis and generates validated reports, enabling teams to ship code securely and confidently.

Hidden Risks in AI-Driven Development

In December, a new vulnerability was discovered that affects most major commercial AI coding apps, where hidden instructions placed inside normal project content—such as comments, commit messages, or pull requests—can trick AI systems into executing harmful actions. AI systems often have high privileges within tools like GitHub. An adversary can slip malicious text into a workflow and cause the AI to run commands, leak sensitive information, or modify code without directly breaching the system. While some vendors have patched specific instances, the core issue lies in the way AI models interpret content, making this a widespread and ongoing security concern.

Looking Forward to 2026

The evolution of the threat landscape through 2026 is likely to follow a similar trajectory to 2025, with greater intensity. State actors are expected to increase activity while shifting toward low noise, high persistence tradecraft. Geopolitical targeting will continue to move from being the exception to the rule in APT activity. Identity-centric and third-party attacks are likely to accelerate, and the role of artificial intelligence will remain both an enabler and an ongoing source of risk.

For executive leadership, the central issue is not simply the volume of attacks. It is the growing persistence of adversaries, the concentration of operational dependencies, and the compression of response timelines. Cybersecurity must be considered in the context of operational resilience and enterprise risk, not solely as a technical function.

Geopolitics, APTs and State Action

Geopolitical competition is very likely to increase through 2026 as trade negotiations evolve and regional powers continue to assert themselves. In this environment, state aligned actors can be expected to execute cyber and cybercrime operations in support of national policy objectives, economic leverage and strategic reconnaissance.

The focus of these actors is shifting from short term financial gain or isolated espionage toward sustained access. Low-noise, high-persistence activity is intended to establish long term footholds in strategically valuable environments. These footholds may support surveillance, intellectual property collection, economic advantage, or pre-positioning for disruption if geopolitical conditions deteriorate.

Critical infrastructure sectors, particularly telecommunications, energy, transportation and industrial environments, remain especially attractive due to their systemic importance. However, organizations outside of traditional critical infrastructure should not assume they are out of scope. Enterprises embedded in strategic supply chains, advanced technology ecosystems or globally exposed markets may also face sustained targeting.

The risk profile in this environment is defined less by immediate disruption and more by prolonged exposure and the potential for service degradation or operational interruption at moments of strategic significance.

Executive Considerations

Organizations should evaluate their true level of cyber resilience and their ability to continue operating during unpredictable and potentially extended service interruptions. This includes:

- Assessing whether critical business functions can operate in degraded conditions
- Integrating cyber exposure into broader geopolitical and enterprise risk discussions
- Shifting from a prevention focused mindset to one that emphasizes resilience and continuity
- Recognizing that persistent targeting may be the norm rather than the exception

Identity Centric and Third-Party Attacks

Trusted third parties, critical identity platforms and shared service providers that operate outside the organization are likely to remain priority targets. Through social engineering, credential compromise, traditional breaches or exploitation of service vulnerabilities, threat actors may seek to compromise entities that provide broad operational access or systemic value.

Identity platforms in particular now function as enterprise critical infrastructure. Disruption or compromise of authentication and access management systems can rapidly affect multiple business units and external customer interactions.

Similarly, incidents affecting key vendors can cascade into operational disruption, regulatory exposure and reputational damage, even if the originating breach occurs entirely outside the organization's own environment.

As organizations centralize services to drive efficiency and cost control, they also concentrate risk. The extended enterprise has become a primary attack surface.

Executive Considerations

Significant consideration should be given to the organization's ability to respond, pivot and continue operating when critical vendors or identity providers suffer an incident.

Leadership should evaluate:

- The business impact of identity platform compromise or outage
- The resilience and transparency of critical third-party providers
- The downstream impact a vendor breach could have on customers and partners
- Whether contingency planning extends beyond internal systems
- Operational agility in the face of third-party failure is increasingly a determinant of enterprise resilience.

AI and the Expanding Risk Surface

Artificial intelligence continues to act as both an enabler and a risk within the cyber landscape.

On the defensive side, AI can materially improve security posture by accelerating detection, supporting scenario planning, enabling more sophisticated testing of environments and enhancing response workflows. Used effectively, it can provide meaningful advantage to security teams.

At the same time, AI lowers the barrier to entry for cyber-attacks. It can assist in code development, guide threat actors through attack methodologies, enhance social engineering and allow less capable actors to execute more sophisticated campaigns. This reduces the time between vulnerability discovery and exploitation and increases the scale at which attacks can occur.

In parallel with its impact on security operations, the deployment of AI solutions across the enterprise introduces its own risk profile. Like any major technology shift, AI systems present vulnerabilities, configuration challenges, data governance concerns and issues related to content generation and publication.

As AI systems gain greater autonomy and deeper integration into sensitive environments, they become high value targets and potential attack vectors. The question is no longer simply what comes next in the industry, but what expanded exposure accompanies that evolution.

Executive Considerations

Leadership should consider:

- How AI systems are governed, monitored and secured as they scale
- The sensitivity of data accessible to AI platforms
- The potential operational and reputational impact of AI misuse or compromise
- Whether innovation velocity is aligned with governance maturity
- AI adoption is a strategic decision that must be accompanied by deliberate risk management.

Strategic Insight

The key to the 2026 threat landscape is the intensification of existing dynamics. State actors will continue to pursue persistent access, operational dependencies will continue to concentrate risk, and AI will continue to accelerate both defense and attack. The defining characteristic of the coming year is sustained pressure rather than isolated disruption.

The leadership challenge is not predicting the next specific attack technique. It is ensuring that the organization can operate, adapt and maintain stakeholder confidence in an environment where persistence, interdependence and acceleration define the threat landscape.

Cybersecurity in 2026 should be understood as a component of enterprise resilience and strategic risk management. Organizations that align security, operations and executive oversight will be better positioned to withstand disruption and compete effectively.

04 How KPMG can Help

KPMG in Canada's Cyber Security practice provides organizations with comprehensive support to detect, respond to, and recover from cyber incidents. Our specialists bring deep experience in incident response, digital forensics, threat intelligence, and recovery operations, helping organizations secure evidence, understand the scope of an incident, mitigate risks, and support internal, legal, and law enforcement requirements.

We work with clients to strengthen their ability to manage and protect critical data across an evolving threat landscape. Our approach views cyber security as a continuous, adaptive capability aligned to business objectives, focused on long-term resilience and sustained value. Our goal is to help you protect your future and create opportunities for secure growth.

KPMG Cyber Security Solutions include:

Incident response readiness and planning
Enhances organizational preparedness through tailored incident response strategies, playbooks, and exercises. This ensures teams are equipped to respond quickly and effectively when a security incident occurs.

Digital investigations and remediation
Provides forensic analysis and incident remediation support to determine what happened, how it occurred, and when appropriate, who was involved. Our work supports containment, eradication, and recovery efforts.

Threat intelligence
Delivers insights into emerging threats, industry-specific risks, and adversary behaviors, helping organizations prioritize assets, strengthen defenses, and reduce the cost and complexity of proactive security.

Data identification and remediation
Uses leading technologies to identify sensitive information, classify and remediate redundant or obsolete data, and support secure information lifecycle management.

Managed Detection and Response (MDR) Services
Combines advanced detection technologies with 24/7 monitoring and threat analysis to accelerate detection and response. Guided investigation and automated response capabilities help organizations contain threats before they result in significant disruption or data loss.

05 Contributors

Incident Response

Kyle Meyers

Kyle Johnston

Anne Labbe

Jordan Michallet

Xaiver Normand

Robin Penrat

Mansoor Haqanee

Chris Walker

Cyber Threat Intelligence

Mike Rosenlund

Aindrea Skelly

06 Contact Us

Incident Response

Alexander Rau
Partner
alexanderrau@kpmg.ca

Guillaume Clement
Partner
guillaumeclement@kpmg.ca

Chris Walker
Partner
chriswalker2@kpmg.ca

Anne Labbé
Senior Manager
alabbe@kpmg.ca

Xavier Normand
Senior Manager
xnormand@kpmg.ca

Mansoor Haqanee
Manager
mhaqanee@kpmg.ca

Cyber Threat Intelligence and Exploited Vulnerabilities

Robert Moerman
Partner
rmoerman@kpmg.ca

Mike Rosenlund
Senior Manager
mrosenlund@kpmg.ca

kpmg.ca