F12.net™

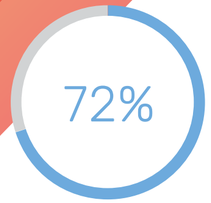
Cybersecurity Trends Report in Canada (2024-2029)

Executive Summary

Rising Cyber Threats

Cyber attacks remain a top concern for Canadian mid-size businesses, with cyber risks ranked as the number one threat to growth in 2024. Nearly three-quarters of small and mid-sized businesses reported a cyber attack in the past year, a significant increase over 2023. According to Insurance Business Magazine, cyber threats dominate concerns for Canadian businesses, with ransomware and phishing being particularly pervasive, causing operational disruptions and financial losses.

Calvin Engen is the Chief Technology Officer at F12.net, where he drives the strategic delivery of secure and scalable IT solutions. With deep expertise in cybersecurity and digital transformation, he focuses on bridging the gap between evolving technology and business resilience. Passionate about protecting organizations from modern cyber threats, Calvin ensures businesses stay ahead in an ever-changing digital landscape.



72% of Canadian SMBs reported being attacked by cybercriminals in the past year, up from 63% a year prior.

Evolving Attack Techniques

Ransomware gangs are escalating tactics – leveraging double-extortion (data theft plus encryption) and even targeting software supply chains. According to Verizon's 2024 Data Breach Investigations Report, breaches involving a third party—such as a supplier or partner—accounted for 15% of all breaches, marking a 68% year-over-year increase. Threat actors are also using AI to craft more convincing phishing lures and automate attacks, as documented in CrowdStrike's research on AI-driven threats.

> The cyber threat landscape in Canada is evolving at an unprecedented pace. Mid-sized businesses, which form the backbone of our economy, are now facing the same level of cyber risk as large enterprises—but often without the same resources. The key to resilience lies in proactive security strategies, from zero trust adoption to continuous threat monitoring. It's not about if an attack will happen, but when—and how well you're prepared to respond.
>
> **Calvin Engen, CTO F12.net**

Key Statistics (2024)

Ransomware

28% of organizations faced a successful attack in the last 12 months.[1]

79% of those victims paid the ransom.

Phishing

66% of Canadian organizations experienced at least one successful attack.[2]

from 82%

Cloud Security

12% of cloud security incidents caused by misconfigurations.[3]

Organization

Medium-sized firms are more likely to be impacted by cyber incidents (**36%**) than smaller businesses (**20%**) according to Insurance Business Magazine.[4]

Increasing Costs and Regulatory Pressure

The cost of cyber incidents is rising. Statistics Canada reports that total recovery spending by Canadian businesses doubled from 2021 to 2023. Cyber insurance uptake is high (around 66–82% of mid-size firms have coverage), but premiums have increased and insurers demand stronger controls, according to Aon's market insights. New data privacy regulations (e.g. Bill C-27's proposed Consumer Privacy Protection Act) promise steep fines (up to 5% of global revenue) for non-compliance, raising the stakes for mid-size companies.

Priorities for the Next 5 Years

Mid-size companies must bolster their cyber resilience. The Canadian Centre for Cyber Security recommends implementing robust ransomware defenses (offline backups, incident response plans), enhancing phishing training and email security, and securing cloud deployments through best practices. Businesses should prepare for forthcoming privacy laws and consider AI both as a threat (e.g. deepfake scams) and a defense (AI-driven threat detection).

Benchmarking against larger enterprises reveals gaps – for example, KPMG research shows ~70% of mid-size firms lack dedicated cybersecurity personnel. Closing these gaps via investment, outsourcing expertise, and adopting frameworks (like zero-trust and NIST guidelines) will be critical to stay secure through 2029.

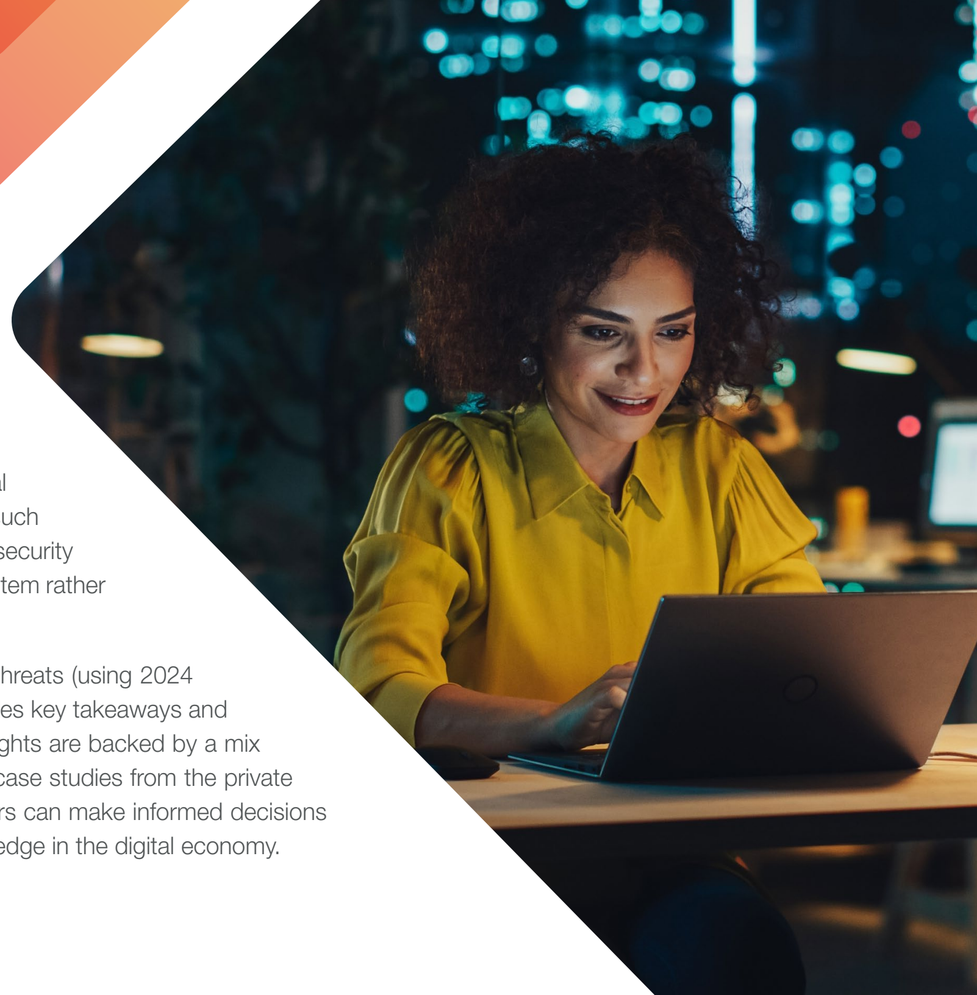
Introduction

Mid-sized companies (typically 50–499 employees) form the backbone of Canada's economy, but they are increasingly in the crosshairs of cyber attackers. In 2024, cyber threats have grown in frequency and sophistication, affecting organizations across all sectors. Business leaders have taken notice: cyber risk was the top concern for 65% of Canadian executives in 2024, ahead of economic uncertainty, according to KPMG's analysis of the Canadian mid-market. High-profile ransomware attacks on hospitals, municipalities, and supply chain partners regularly make headlines, underscoring that no organization is immune.

This report examines key cybersecurity trends impacting mid-size Canadian businesses, drawing on data from the past year (2024) and looking ahead five years. We focus on eight critical areas: ransomware, phishing, cloud security, regulatory compliance, AI-driven threats, emerging attack vectors, cyber insurance, and benchmarking by company size. For each, we present high-level insights, relevant statistics, and real examples to inform strategic decision-making. The goal is to equip business leaders with an understanding of the evolving threat landscape and practical knowledge to strengthen their organization's cyber defenses.

Despite often having fewer resources than large enterprises, mid-size firms handle valuable data and operations that make them attractive targets. They also frequently collaborate with larger organizations, meaning a security incident can have cascading impacts through supply chains. On the positive side, many mid-market companies are investing more in cybersecurity than ever. KPMG surveys show that 81% of Canadian SMB leaders now consider cybersecurity a critical business priority requiring bold action. Yet challenges remain, such as talent shortages (70% of these firms lack in-house cybersecurity expertise) and the tendency to treat cybersecurity as a checklist item rather than a continuously managed risk.

In the sections that follow, we detail the current state of cyber threats (using 2024 data) and explore projections through 2029. Each section includes key takeaways and recommended practices tailored to mid-size enterprises. All insights are backed by a mix of sources, from government research and industry surveys to case studies from the private sector. By understanding these trends, mid-size business leaders can make informed decisions to protect their companies' assets, reputation, and competitive edge in the digital economy.



Ransomware Trends

Ransomware continues to be one of the most disruptive cyber threats to mid-size organizations. Attackers infiltrate a network, encrypt critical data, and demand payment (often in cryptocurrency) for the decryption key – and increasingly, they threaten to leak stolen data (the "double extortion" tactic). The Canadian Centre for Cyber Security estimates that ransomware is "almost certainly the most disruptive form of cybercrime", with greater impact today than in 2020. 2024 saw ransomware groups refining their methods and expanding their targets:

Higher Frequency of Attacks

Industry surveys indicate a sharp rise in ransomware incidents among mid-market firms. Nearly three-quarters (72%) of Canadian SMBs reported being attacked by cybercriminals (primarily via ransomware) in the past year, up from 63% a year prior, according to Genatec's survey data. Another study found 76% of mid-sized businesses (50-249 employees) experienced a ransomware attack in the past year, slightly higher than the rate for large enterprises (70%).

Soaring Ransom Payments

Unfortunately, many victims still pay. KPMG reports that over two-thirds (67%) of Canadian SMB leaders admit their company paid a ransom in the last three years. In 2024 specifically, of the organizations that suffered a ransomware breach, 46% paid the attackers' demands. Ransoms can be steep – nearly one-third of payments by businesses were between $1 million and $5 million. These payouts fuel the ransomware economy, incentivizing criminals to continue and even embolden them to target new victims.

Supply Chain **Attacks on the Rise**

A notable trend is ransomware entering organizations via their software providers or contractors. In OpenText Cybersecurity's 2024 Ransomware Survey, 62% of respondents hit by ransomware said the attack originated from a compromise in their software supply chain. This was evidenced by incidents like the breach of a major software vendor that impacted thousands of its client companies. Mid-size firms are often connected to larger enterprises or critical networks, making them attractive pivot points for attackers – they may have weaker defenses but provide a foothold into broader ecosystems.

Financial impact: In 2024, the average ransomware payment from Canadian mid-size businesses exceeded $800,000, with many companies facing additional costs in lost revenue, recovery efforts, and reputational damage.

Escalating Tactics

Ransomware groups are using more aggressive techniques to force payment. Beyond data encryption, many now engage in data theft and threaten public leaks of sensitive information, causing reputational damage. They also target backups and cloud storage (to prevent victims from restoring data) and have even harassed victims' customers or partners for added pressure. The Canadian national cyber threat assessment warns that over the next two years, ransomware actors will "almost certainly escalate their extortion tactics" to increase pressure to pay.

Impact on Operations and Reputation

The immediate effect of a ransomware attack is downtime – systems locked up, business operations halted. For mid-size companies, even a few days of outage can be devastating. In 2024, BNN Bloomberg reported that 44% of Canadian organizations experienced a cyber attack of some kind, and 28% of those said the incident negatively impacted their reputation. Customers and partners may lose trust, especially if personal data is leaked. Notably, 74% of security professionals surveyed in Canada support making it illegal to pay ransoms, reflecting a view that ransom payments only perpetuate the problem.

Best **Practices**

Mid-size businesses should approach ransomware as a when-not-if scenario. Key defenses include:

Backup Strategy: Maintain offline, encrypted backups of critical data and test restore procedures regularly.

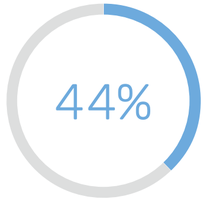
Network Segmentation: Implement strong separation so an intruder can't easily move laterally.

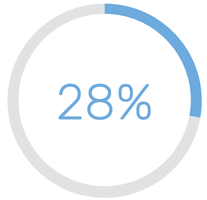
Patch Management: Ensure all systems are updated to close known vulnerabilities commonly exploited.

Employee Education: Since many attacks start with phishing, train staff to recognize suspicious emails.

Incident Response Plan: Develop and practice procedures specifically for ransomware scenarios.

KPMG's cybersecurity report notes that 66% of SMBs admit they have no formal plan for ransomware incidents. Developing such plans and practicing them (e.g. via tabletop exercises) can significantly reduce response time and damage when an attack hits.





44% of Canadian organizations experienced a cyber attack of some kind, and 28% of those said the incident negatively impacted their reputation.

Phishing and Social Engineering

Phishing remains the most prevalent cyber threat vector, especially for mid-size organizations. These attacks typically involve deceptive emails (or texts and phone calls in the case of “smishing” and “vishing”) that trick employees into clicking malicious links, divulging passwords, or executing malware. Despite years of user education efforts, phishing continues to succeed at an alarming rate:

Prevalence of Phishing Breaches

Roughly two-thirds of Canadian organizations (66%) suffered at least one successful phishing attack in 2023, according to Proofpoint’s 2024 State of Phish Report. (This was actually a slight improvement from 82% the year before, possibly due to increased awareness). Phishing is implicated in a large share of security incidents – by one estimate, 74% of data breaches involve a “human element” such as falling for phishing or using stolen credentials. In mid-size companies, where employees often wear many hats, attackers bank on someone eventually clicking a booby-trapped email if enough are sent.

Business Email **Compromise** (BEC)

A particularly damaging form of phishing is BEC, where fraudsters impersonate a CEO or trusted vendor and trick staff into sending large wire transfers or sensitive data. Mid-size firms have been swindled out of hundreds of thousands of dollars in such schemes, which often do not involve malware and thus bypass technical defenses. BEC attacks surged in recent years globally, and Canadian firms are not spared – the FBI reports BEC as the costliest cybercrime worldwide. Mid-size companies should be wary of any urgent, atypical payment requests via email.

Employee Risk **Behavior**

Worryingly, many employees still engage in risky behaviors. In Proofpoint’s 2024 survey, 67% of Canadian employees admitted to knowingly clicking links or opening attachments that could pose security risks. This suggests that awareness of phishing doesn’t always translate into caution in practice. Common phishing lures seen in 2024 included fake voicemail notifications, shipment delivery notices, cloud document share links, and urgent “security alert” emails prompting password resets. Attackers craft messages that appear legitimate and time-sensitive to lower employees’ guard.

Phishing insight: The most successful phishing emails create a sense of urgency that bypasses rational thinking. Training should emphasize “stop and verify” practices for any request involving credentials, payments, or sensitive information.

Impact and Consequences

The fallout from a successful phishing attack can be severe. Clicking a malicious link may deploy ransomware (locking up the network) or lead to a stealthy breach where data is stolen. BNN Bloomberg reported a 326% increase in financial penalties (regulatory fines) related to phishing-driven breaches in 2024 – likely reflecting stricter enforcement of privacy laws after data leaks. Additionally, if attackers steal email account credentials, they can launch internal phishing ("thread hijacking") from a legitimate account, making detection even harder. Phishing is often the first domino in a chain of compromise.

Training and Culture

Most mid-size businesses conduct security awareness training, but frequency and effectiveness vary. Around 91% of organizations now require employees to attend cybersecurity or phishing training. However, simply running annual training may not be enough – many firms still treat it as a compliance checkbox. In fact, KPMG found that 71% of Canadian SMBs acknowledge their cyber awareness training is "tick-the-box" and not deeply ingrained. Progressive companies are moving toward more frequent, engaging training (e.g., quarterly phishing simulations – which 66% of organizations did by 2024). The goal is to foster a culture of skepticism where employees double-check unusual requests and feel accountable for security.

Best **Practices**

To combat phishing, mid-size companies should deploy a combination of technology and education:

Technical Safeguards: Email security filters, Multi-factor authentication, Endpoint protection

Deploy advanced email filtering to block known threats; Require MFA on all remote access and email accounts; Install endpoint protection that can detect malware from clicked links.

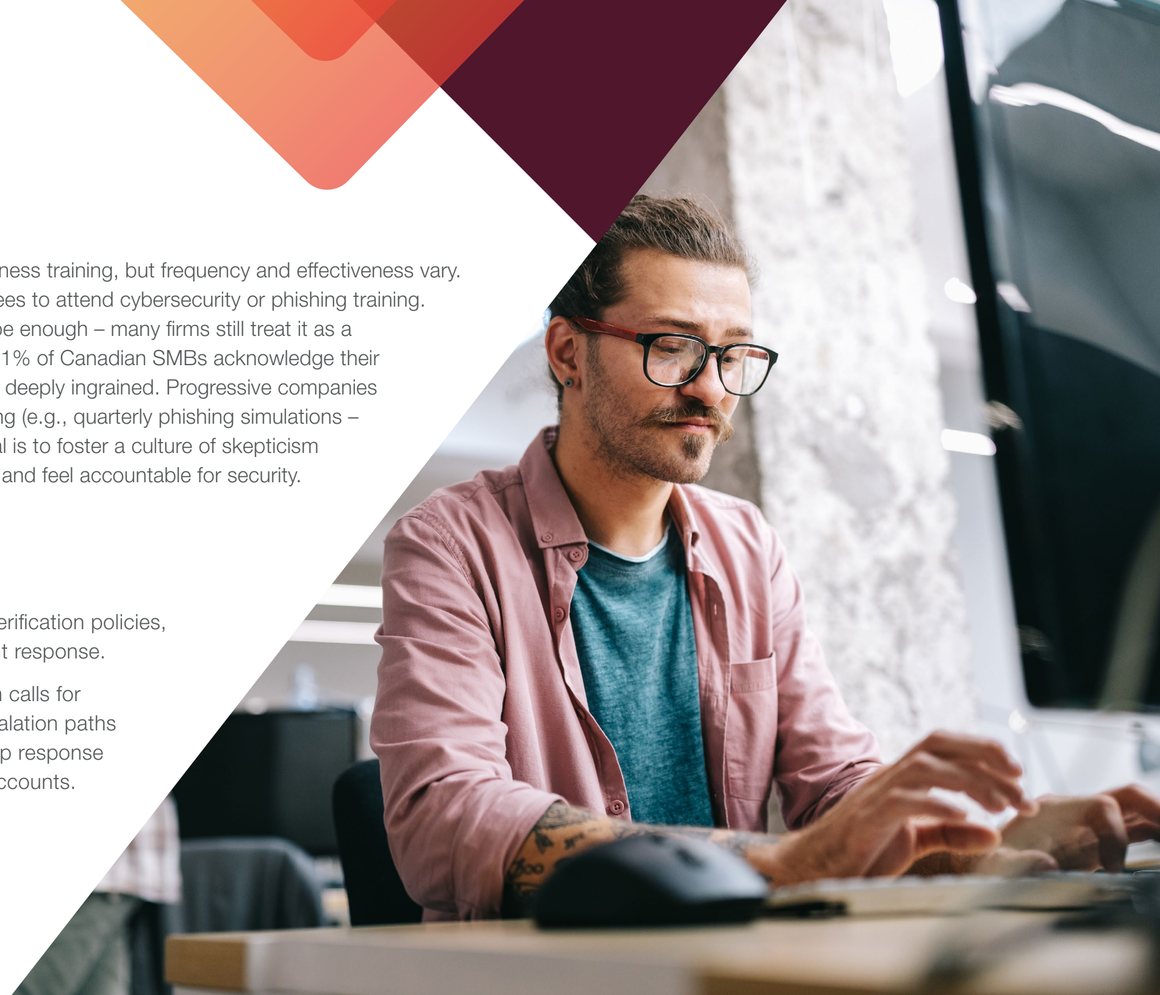
Employee Training: Phishing simulations, Awareness programs, Verification procedures.

Run quarterly simulated phishing campaigns; Use real-world examples in training; Create quick reporting mechanisms for suspicious emails.

Process Controls: Payment verification policies, Data transfer protocols, Incident response.

Establish mandatory verification calls for wire transfers; Create clear escalation paths for suspicious requests; Develop response procedures for compromised accounts.

Many organizations are turning to simulated phishing campaigns to continually test and train employees in a safe setting. It's crucial to establish clear policies, such as procedures for verifying any payment requests or data transfers (e.g., always call the requester on a known phone number before transferring funds). By reinforcing these habits and implementing robust email security, companies can significantly reduce their phishing risk.



Cloud Security:
Challenges and Best Practices

Mid-size companies have widely embraced cloud services (such as Office 365, Google Workspace, and various SaaS and cloud infrastructure platforms) for their agility and cost-effectiveness. However, moving data and applications to the cloud introduces new security challenges. In 2024, misconfigured cloud resources, insufficient access controls, and gaps in monitoring were among the leading causes of breaches. Key trends include:

Misconfigurations and Human Error

Misconfigurations remain a critical weak point in cloud security. According to the 2024 Cloud Security Report by Check Point, configuration and management errors were responsible for 12% of all cloud security incidents—allowing attackers to exploit exposed storage, weak access controls, and policy gaps that leave organizations vulnerable. Small IT teams in mid-size firms may lack deep cloud expertise, which can lead to errors. Regular audits and automated configuration checks are increasingly seen as critical.

Rising **Cloud Attacks**

As businesses migrate more workloads to the cloud, attackers are following. Four out of five companies reported an increase in the frequency of attacks on their cloud environments, with common attack types including data breaches (33% of cloud attacks), cloud account compromises, and even illicit cryptocurrency mining in cloud instances. In Canada, several high-profile data exposures in 2024 were tied to cloud storage missteps – for instance, databases left unsecured by third-party partners. Mid-size firms need to realize that “the cloud” is not automatically secure by default; security remains a shared responsibility.

Access Management and Credentials

Phishing for cloud account passwords and abusing stolen credentials has become one of the top tactics. Over half of organizations say phishing for cloud logins is among the most prevalent attack methods. Once an attacker gains a cloud admin account, they can access vast amounts of data. Strong identity and access management (IAM) is therefore paramount. This includes enforcing MFA, using role-based access with least privilege (ensuring employees only have the cloud permissions they need), and promptly revoking access when people change roles or leave.

Cloud security tip: Identity is the new perimeter in cloud environments. Implementing robust identity and access management with multi-factor authentication can prevent 99.9% of account compromise attacks.

Data Protection and Compliance

Storing customer data in cloud services raises concerns about privacy and regulatory compliance. Companies must ensure data is encrypted (in transit and at rest) and properly backed up. With laws like Canada's proposed Bill C-27 (and existing provincial privacy regulations), mid-size firms will be expected to protect personal information in the cloud just as diligently as on-premise. Notably, cloud providers offer many native security features – encryption, audit logs, region-based data residency options – but it's on businesses to configure and use them correctly.

Cloud Security Investments

Encouragingly, mid-market organizations are ramping up cloud security efforts. In 2024, 62% of SMB respondents reported increasing their investment in cloud security tooling and expertise (up from only 39% two years prior). Common best practices include deploying Cloud Access Security Broker (CASB) solutions to gain visibility into cloud usage, monitoring and alerting for unusual cloud activities (e.g., impossible travel logins or large data downloads), and regular cloud security assessments or penetration tests. Many companies are also embracing frameworks like zero-trust, which treat every access request as untrusted by default, whether it originates inside the corporate network or from the cloud.

Best **Practices**

To secure cloud assets, mid-size businesses should establish a cloud governance model. Key steps:

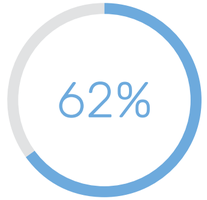
Implement MFA and strong IAM policies for all cloud accounts.

Continuously monitor cloud configurations using tools or managed services that can flag misconfigurations (many breaches are preventable with the right alerts).

Encrypt sensitive data and manage your encryption keys carefully (consider customer-managed keys for critical data).

Regularly back up cloud data to a separate, secure location, and test restore processes.

Train staff on secure cloud practices, including how to recognize cloud-specific phishing scams (e.g., fake login pages).



In 2024, 62% of SMB respondents reported increasing their **investment in cloud security tooling and expertise.**

Additionally, ensure contracts with cloud providers outline security responsibilities and that you maintain visibility into what the provider is doing to protect the infrastructure. By following a shared responsibility approach, mid-size enterprises can leverage the cloud's benefits without compromising security.

Regulatory Compliance and Data Privacy

Cybersecurity for mid-size companies isn't just about technology – it's also about complying with evolving laws and regulations. Canada is in the process of overhauling its privacy and data protection regime, which will impose new obligations on organizations in the coming years. Business leaders need to stay ahead of these changes to avoid fines and maintain customer trust.

Bill C-27 and Federal Privacy Reform

One of the most significant developments is Bill C-27, the proposed Digital Charter Implementation Act. This federal bill (currently pending, as of early 2025) would enact the Consumer Privacy Protection Act (CPPA), replacing Canada's aging PIPEDA law with stronger privacy protections. Under Bill C-27's CPPA, mid-size companies would be required to implement a comprehensive privacy management program and could face heavy penalties for violations – up to $25 million or 5% of global revenue for serious infractions. For example, failing to obtain valid consent or inadequate safeguarding of personal information could result in fines. Bill C-27 also includes the Artificial Intelligence and Data Act (AIDA), introducing rules for high-impact AI systems (important for companies deploying AI). Although Bill C-27 was delayed in Parliament, it signals where regulations are heading: stricter requirements around data consent, transparency, breach notification, and accountability.

Provincial Laws (e.g., Québec's Law 25)

In addition to federal law, provinces are raising the bar on privacy. Québec's Law 25 (formerly Bill 64) is a recent example – it modernizes provincial privacy rules and has phased in new requirements between 2022 and 2024. Any company (even outside Québec) handling Québec residents' personal data must comply. Law 25 mandates measures such as appointing a privacy officer, conducting privacy impact assessments for sensitive projects, and reporting data breaches to the regulator and affected individuals. It also introduced fines up to CAD $10 million or 2% of worldwide turnover for non-compliance. Other provinces, like British Columbia and Alberta, have their own private-sector privacy laws, and Ontario has been considering one. Mid-size firms operating across Canada need to navigate this patchwork and perhaps adhere to the highest standard across jurisdictions.

Compliance alert: Recent amendments to Canada's privacy laws have shortened the timeline for breach notifications. Organizations now face stricter deadlines and must be prepared to respond quickly with the right information for regulators and affected individuals.

Data Breach Notification

Under both current and proposed laws, organizations have a duty to report certain cyber incidents. PIPEDA already requires companies to report breaches that pose a “real risk of significant harm” to individuals to the Privacy Commissioner and to notify affected individuals. Bill C-27’s CPPA would maintain and potentially strengthen this. Law 25 in Québec also requires prompt notification to the regulator (the CAI) for any confidential information breach. Beyond legal requirements, timely and transparent communication after a breach is considered best practice to maintain trust.

Compliance as a Competitive Advantage

Rather than viewing regulations as a burden, many mid-size businesses are starting to treat strong cybersecurity and privacy as a selling point. With cyber incidents causing reputational damage (28% of organizations said a cyber attack hurt their reputation in 2024, according to BNN Bloomberg), demonstrating good stewardship of data can win customers. For instance, implementing frameworks like ISO 27001 or obtaining cybersecurity certification (such as the federal CyberSecure Canada certification for SMBs) can signal a company’s commitment to security. Additionally, cyber insurance providers often look favorably on companies with mature compliance programs.

Preparing for the **Next 5 Years**

Looking ahead, we expect more regulatory activity. If Bill C-27 (or a similar successor) is enacted by 2025, mid-size companies will need to align their policies with its requirements – updating privacy policies, refining consent mechanisms (especially around any AI-driven data processing), and ensuring the ability to honor individuals’ rights (like data deletion requests). Enforcement of privacy laws is likely to increase, with regulators levying larger fines for negligence. Also, sector-specific regulations may emerge (for example, critical infrastructure operators now face cybersecurity baseline requirements under Canada’s Bill C-26). Mid-size firms should track guidance from government bodies like the Office of the Privacy Commissioner and the Canadian Centre for Cyber Security. By instituting a culture of compliance – regular training on data handling, keeping records of data flows, and conducting security audits – companies can reduce legal risk while also mitigating chances of a breach.

Key **Takeaway**

Regulatory compliance is becoming an integral part of cybersecurity risk management. Mid-size businesses should proactively invest in privacy and security controls now, rather than wait for enforcement. This means keeping an inventory of what personal data you hold, where it’s stored (on-premise or cloud), and how it’s protected. Conduct gap assessments against upcoming laws (such as checking if your consent forms and processes meet CPPA standards). Engaging legal counsel or privacy consultants to prepare for laws like Bill C-27 can be worthwhile. Ultimately, organizations that bake compliance into their operations – aligning people, processes, and technology with privacy principles – will be better positioned to avoid penalties and thrive in the trust-driven digital marketplace

AI-Driven Cybersecurity
Threats and Defenses

Advances in artificial intelligence are a double-edged sword for cybersecurity. On one side, cyber criminals are exploiting AI tools (especially generative AI) to launch more sophisticated attacks; on the other, defenders are leveraging AI to detect and respond to threats faster. For mid-size businesses, understanding this evolving landscape is crucial, as AI can amplify both offense and defense.

Malicious Use of Generative AI

In 2024, threat actors widely adopted AI-based tools to enhance social engineering. For example, AI-driven phishing has become common – attackers use generative AI (like advanced language models) to craft highly convincing spear-phishing emails that are grammatically perfect and tailored to the target according to CrowdStrike research. This makes phishing harder to spot. AI chatbots can even conduct real-time interactions with victims via text or email, impersonating customer support or vendors in a near-human manner. There have also been cases of deepfake audio used in fraud (impersonating a CEO's voice over the phone to authorize a fake transfer). With AI, criminals can scale their operations – auto-generating scam emails, fake websites, or bogus news to trick users at a volume and personalization level not seen before.

AI-Powered Malware and Evasion

Attackers are beginning to employ AI to improve malware. Machine learning can help malware dynamically adapt or choose the best exploit methods for a given environment. AI might also be used to evade detection – for instance, by generating polymorphic code that constantly changes signature, or by finding blind spots in AI-based threat detection systems (through adversarial examples that fool ML classifiers) according to the Canadian Centre for Cyber Security. While still early, security experts anticipate the next five years could see "smart malware" that reacts to defenses in real time.

AI defense potential: AI-powered security tools can process threat data 60x faster than human analysts and identify patterns across billions of data points, making them particularly valuable for mid-size companies with limited security staff.

AI in **Defense**

On the positive side, mid-size companies have new tools in their arsenal as cybersecurity vendors embed AI into their products. AI-driven security systems (often marketed as using machine learning or “User and Entity Behavior Analytics”) can sift through large volumes of network data to identify anomalies – potentially catching attackers who have slipped past traditional filters. For example, an AI system might flag an employee account that suddenly downloads an unusual amount of data at 3 AM, enabling a quicker incident response. Many mid-size firms are considering these capabilities: KPMG reports that 79% of SMB leaders said they are looking at using AI to bolster cybersecurity. In practice, this includes tools like AI-assisted email filtering, automated incident response playbooks, and threat intelligence platforms that use AI to predict attack patterns.

Generative AI for Defense

Some organizations are experimenting with generative AI assistants to help cybersecurity staff. These AI assistants can help analyze suspicious files or network logs, draft responses to incidents, or even generate training content (like custom phishing simulation emails). However, caution is needed – feeding sensitive data into third-party AI services can itself be a risk if not handled properly. More broadly, there is a talent gap in cybersecurity, and AI tools might augment limited human teams (common in mid-size companies) by automating routine tasks.

Concerns and Governance

Understandably, there is concern about the security implications of AI. A Canadian survey found 70% of cybersecurity professionals are worried about how generative AI could amplify cyber threats. Yet at the same time, 57% of organizations reported they have started integrating AI tools into their cybersecurity operations (up from 44% in 2023). This highlights a rapid adoption curve, but also the need for governance – companies should set guidelines for safe AI usage, ensuring that any AI systems (internal or vendor-provided) are tested for biases and adversarial vulnerabilities. New regulations like the AIDA (if enacted via Bill C-27) may also require assessments of AI systems’ impacts on privacy and security, adding another compliance dimension.

Best **Practices**

Mid-size businesses should approach AI in cybersecurity strategically:

For defensive AI tools – treat them as supplements, not replacements, for skilled staff.

Verify vendor claims and understand the AI’s limitations (can it explain its decisions?).

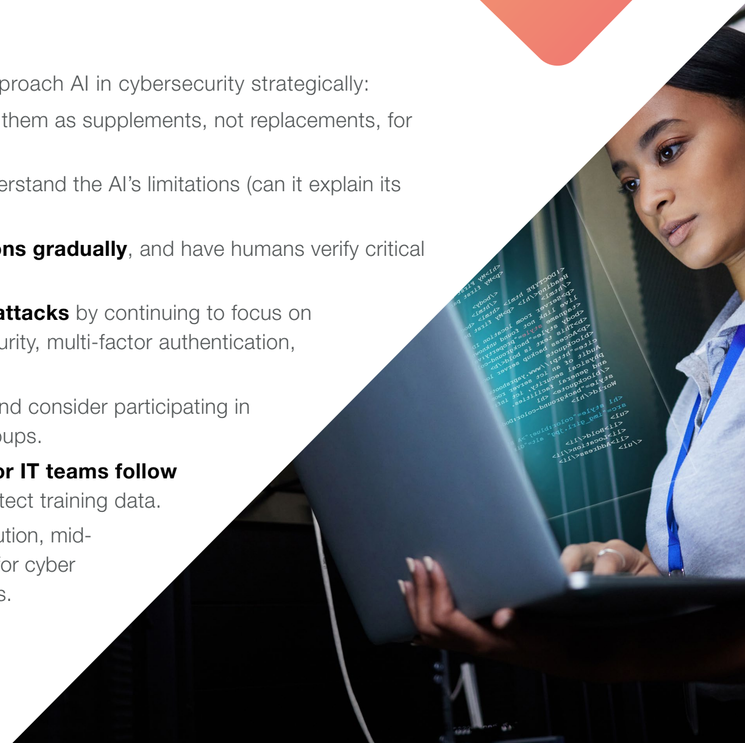
Incorporate AI-driven solutions gradually, and have humans verify critical outputs.

Guard against AI-enhanced attacks by continuing to focus on fundamentals: robust email security, multi-factor authentication, and verification procedures.

Stay informed on AI trends and consider participating in industry information-sharing groups.

Ensure your data scientists or IT teams follow ethical AI guidelines, and protect training data.

By balancing innovation with caution, mid-size companies can harness AI for cyber defense while minimizing its risks.



Emerging Attack Vectors
Targeting Mid-Size Businesses

Beyond phishing and ransomware, several other cyber-attack vectors are emerging (or re-emerging) as significant threats to mid-size organizations. Attackers are constantly innovating, probing for any weak link. Here are some trends to watch:

Supply Chain and Third-Party Attacks

As noted earlier, attackers are breaching smaller suppliers to reach larger targets – and vice versa. Mid-size companies often sit in the middle of supply chains, making them a perfect stepping stone. OpenText Cybersecurity's 2024 Ransomware Survey found that 91% of organizations voiced concern about attacks on their software supply chain. Real-world example: in 2024, a ransomware group exploited a vulnerability in a popular IT management software – mid-size firms using that software were encrypted en masse, and some of their enterprise clients had data access disrupted. Mitigating supply chain risk involves vetting vendor security (74% of companies have a process to assess supplier cybersecurity, but a quarter do not) and insisting on standards in contracts.

Business Email Compromise (BEC) & Fraud

BEC scams were mentioned under phishing, but it's worth re-emphasizing as a distinct threat. Unlike mass phishing, BEC schemes are highly targeted and may involve weeks of reconnaissance. Attackers often study a mid-size company's org chart (via LinkedIn, etc.), compromise a real email account or register a lookalike domain, and then trick someone in finance into sending a payment. These attacks bypass technical defenses because they contain no malware – just social engineering. Losses can be devastating and often not insured if negligence is found. Regular staff training and strict financial controls (e.g., requiring multiple approvals for transfers, verifying changes to vendor payment info by phone) are key.

Insider Threats

While external hackers dominate the news, insiders (disgruntled employees, or careless ones) are an ongoing risk. A mid-size business might not have the monitoring tools that large enterprises do to detect suspicious internal activity. Yet consider that employees often have broad access in smaller organizations. 2024 saw cases of insiders stealing data to take to competitors or manipulating systems for personal gain. Companies are increasingly implementing measures like user activity monitoring and stricter least-privilege access internally to counter this.

Attacks on Remote Work Infrastructure

The pandemic-era shift to hybrid work introduced lasting vulnerabilities. Mid-size firms may have many employees who connect from home networks. Attackers exploit this via insecure home routers, or by targeting personal devices that access corporate data. There have been instances of attackers intercepting Wi-Fi traffic or using malware on an employee's home PC to VPN into the company network. Ensuring remote work security (through steps like providing corporate-managed laptops, enforcing VPN usage, and educating staff on home network security) is now part of baseline cybersecurity.

IoT and Operational Technology

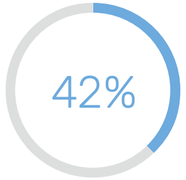
Many mid-size companies, particularly in manufacturing, retail, or logistics, deploy Internet of Things (IoT) devices – from smart thermostats and cameras to industrial control systems. These can be weaker on security (some IoT devices don't get regular patches or use default passwords). Attackers have begun exploiting IoT as entry points. For example, a hacker might breach a building's smart HVAC system and pivot to the corporate network. Similarly, attacks on operational technology (OT) – the systems controlling equipment on factory floors – are rising, as seen in cases where production was halted due to ransomware or wiper malware. Mid-size firms should inventory connected devices and isolate IoT/OT networks from core IT.

DDoS and Extortion

Some threat groups use Distributed Denial-of-Service (DDoS) attacks to overwhelm a company's website or online services, often coupled with extortion demands (pay or stay offline). Mid-size e-commerce and tech firms have been hit by these "ransom DDoS" threats. Cloud-based DDoS protection services are increasingly essential for businesses that rely on internet-facing systems. Even if an organization is not primarily online, an attacker might DDoS their VPN or email server to disrupt operations as part of a broader attack.

Best **Practices**

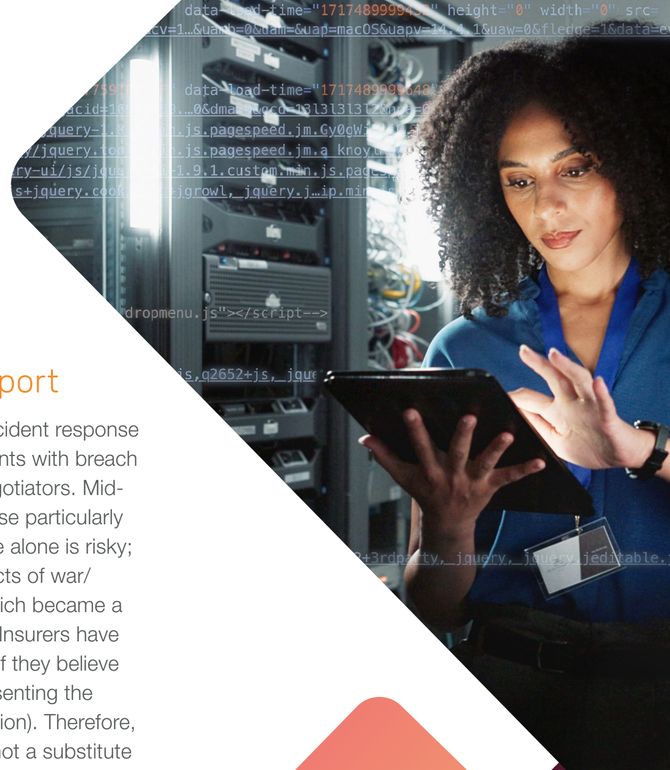
To address these diverse threats, mid-size companies should adopt a proactive, layered security strategy. This includes third-party risk management – vetting the security of vendors and requiring measures like SOC 2 reports or security questionnaires. For fraud and BEC, implement process controls (e.g., callbacks for verification, spending limits). Regularly update and patch all software, including lesser-noticed systems like network gear or IoT device firmware. Employ network segmentation, keeping critical systems and IoT devices on separate networks so a breach in one doesn't immediately compromise all. And consider investing in threat intelligence services or information-sharing communities specific to your industry – early warning about new scams or vulnerabilities can be invaluable. By diversifying their defenses and not just focusing on the headline threats, mid-size businesses can guard against the full spectrum of cyber risks.



Executive alert: Business Email Compromise attacks targeting Canadian organizations increased by 42% in 2024, with an average loss of $117,000 per successful attack, according to BNN Bloomberg.

Cyber Insurance
Trends and Requirements

Cyber insurance has become an important safety net for mid-size companies, helping to offset financial losses from incidents. However, the cyber insurance landscape is rapidly evolving in response to the surge in attacks. Key points for 2024 and beyond:



High Adoption, but Changing Conditions

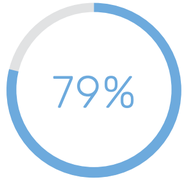
A majority of Canadian mid-size businesses now carry cyber insurance, though statistics vary. A 2024 survey found 66% of business leaders had cyber insurance (down from 72% in 2023, as some dropped coverage due to cost). Another reported that 82% had coverage, up from 59% in 2021, indicating growing interest, according to Insurance Business Magazine. Insurers have tightened underwriting – companies are often required to demonstrate certain security measures in place (like MFA, regular backups, and employee training) to qualify or to get better premiums. In fact, some mid-market firms that treated cybersecurity as a low priority have found their insurance renewal denied or significantly more expensive.

Premiums and **Coverage Limits**

The past few years saw sharp increases in cyber insurance premiums (in the wake of costly ransomware claims worldwide). For many mid-size organizations, premiums doubled or tripled between 2020 and 2022. By 2024, the market shows signs of stabilizing, with insurers adjusting pricing models. Some reports suggest the cyber insurance market is “softening” slightly for first-time buyers with good controls according to Aon’s market insights. Still, businesses should budget for substantial costs – but weigh that against potential losses from an incident (which can reach millions). Also, coverage limits might not fully cover a catastrophic breach; firms need to understand any sublimits (e.g., separate limits for ransomware payments or for regulatory fines).

Incident Response Support

One benefit of insurance is access to incident response services. Insurers often have arrangements with breach coaches, forensic investigators, and negotiators. Mid-size companies lacking in-house expertise particularly value this. However, relying on insurance alone is risky; policies have exclusions (for instance, acts of war/cyber-terrorism may not be covered, which became a debate after some high-profile attacks). Insurers have even started suing clients over payouts if they believe negligence was involved (e.g., misrepresenting the state of security controls on the application). Therefore, treating insurance as a supplement to, not a substitute for, sound security practices is critical.



Insurance insight: While cyber insurance premiums have increased by an average of 79% since 2021, organizations with demonstrable security controls like MFA and endpoint protection are seeing premium increases of only 35-45% on average.

Requirements and Compliance for Policyholders

To obtain and maintain coverage, mid-size businesses are increasingly expected to meet certain criteria. Common requirements include: having up-to-date anti-virus/endpoint protection on all systems; evidence of regular data backups (with an offline copy); multi-factor authentication for remote access and privileged accounts; and documented incident response and business continuity plans. Some insurers now ask detailed questionnaires about patch management, employee training frequency, cloud security configurations, etc. Demonstrating compliance with frameworks like NIST or CIS 20 controls can favorably influence underwriters. We've seen that companies which can show a proactive cybersecurity program tend to get more favorable terms.

Claims and Payout **Trends**

Roughly 30% of businesses have experienced some cyber incident according to Statistics Canada, and those with insurance have filed claims for things like ransomware recovery costs, legal liabilities, and notification expenses. Interestingly, even though cyber risk is at all-time highs, some organizations opt to go uninsured – in one survey, 32% of those without cyber coverage cited cost as the main barrier. This points to a need to quantify risk – for many mid-size firms, one serious breach could far exceed the cost of premiums. Additionally, regulators in the future might view lack of insurance as a sign of insufficient risk management (though not a formal requirement, it's becoming a norm in due diligence).

Best **Practices**

If you pursue cyber insurance, treat it as one layer of defense. Shop around with brokers who understand your business sector and can advise on appropriate coverage (including any specialized riders for things like social engineering fraud or system outages). Be candid and thorough in your application – failing to disclose a material fact could void your coverage when you need it most. Once insured, ensure you adhere to the security practices you attested to. Also, leverage the resources insurers provide: incident response planning, training materials, or vulnerability assessments may be included. Finally, keep senior leadership and the board informed about insurance coverage and its limits, as part of overall cyber risk governance. The goal is to strike the right balance: invest in preventing incidents, but have insurance to backstop the unforeseen worst-case scenarios.

Mid-Size vs Large and Small: How Do Threats and Preparedness Compare?

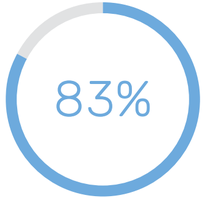
It's useful for mid-size organizations to understand how their cybersecurity posture and threat experience stack up against both smaller businesses and larger enterprises. Some notable comparisons:

Cybersecurity Comparison by Organization Size

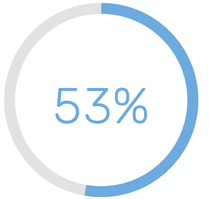
Metric (2024)	Small Businesses	Mid-Size Businesses	Large Enterprises
Experienced a cyber incident in past year	20% Insurance Business Magazine	36% Insurance Business Magazine	30% Statistics Canada
Victim of successful ransomware (12 mo)	(lower) ~20%*	28% BNN Bloomberg	(similar) ~30%*
Paid ransom if attacked (last 3 yrs)	(data n/a)	67% KPMG	(data n/a)
Have cyber insurance coverage	~5%** Aon	66-82% Insurance Business Magazine / BNN Bloomberg	>80% (est.)
Consider cybersecurity a top priority	~60%***	81% KPMG	72% (CEO level)***
Feel prepared for cyber attack	(varies)	83% (self-reported) KPMG	53% (CEOs) KPMG
Lack of skilled cyber personnel	50%***	70% KPMG	20%***

The benchmarking reveals a "cybersecurity middle ground": mid-size companies face threats closer in frequency/severity to large organizations, but often have security budgets and teams more akin to small businesses. For instance, while 76% of mid-sized companies had a ransomware encounter in the past year, most lack dedicated security operations centers or advanced defenses that big corporations deploy. This can make the impact of each incident disproportionately high. It also explains why mid-market firms are increasingly investing in managed security services or outsourcing certain functions to close the gap.

*Notes: Small business data on ransomware is limited, but studies suggest they are targeted slightly less often than mid-size firms, yet attacks can be equally ruinous (94% of SMBs reported cyber attacks in one survey). Large enterprises have more attacks in absolute terms, but also more resources to defend and recover. Only ~16% of all Canadian businesses (including micro firms) reported an impactful cyber incident in 2023 StatCan, reflecting the many very small businesses in the economy. Meanwhile, mid-size and large firms faced a higher likelihood of incidents.



83% of mid-size business leaders believed they were well-prepared for an attack.



53% of large enterprise CEOs felt prepared.

On a positive note, mid-size firms appear to be growing more aware of cyber risks. They outpace small businesses in prioritizing cybersecurity (as shown by the 81% figure considering it critical). In some areas, they even exhibit overconfidence – for example, KPMG found that 83% of mid-size business leaders believed they were well-prepared for an attack, despite many having minimal in-house security staff. In contrast, only 53% of large enterprise CEOs felt prepared, perhaps reflecting a more cautious assessment due to greater exposure and understanding of what sophisticated attacks entail.

The takeaway is that mid-size organizations should neither underestimate their attractiveness to attackers nor overestimate their own preparedness. By learning from the practices of larger enterprises (such as adopting more structured risk management, and leveraging frameworks like ISO/NIST) and addressing the gaps that small businesses struggle with (like lack of expertise and insurance), mid-size companies can position themselves more securely. Benchmarking can inform budget decisions too – e.g., knowing that large firms spend significantly on areas like 24/7 monitoring and incident response, mid-size firms might decide to allocate funds for an external managed detection and response (MDR) service to achieve a similar outcome at a fraction of hiring a full team.

Strategic insight: The “Goldilocks Zone” for mid-size businesses is to adopt enterprise-grade security approaches while maintaining the agility and cost-effectiveness of smaller organizations. This often means leveraging managed security providers rather than building large internal teams.

Conclusion and **Future Outlook**

Cyber threats are an ever-moving target. For Canada's mid-size companies, 2024 underscored that they are squarely in attackers' sights – experiencing breach rates closer to large enterprises, but often without the same defenses. The next five years will likely bring further escalation in threat activity. Ransomware gangs may shift tactics again (perhaps focusing more on data extortion if organizations harden backups, or exploiting emerging tech like quantum-proof encryption gaps once quantum computing advances). Phishing will continue as a primary vector, potentially augmented by AI to be even more convincing. Meanwhile, new frontiers – from attacks on cloud APIs to assaults on AI systems themselves – could emerge.

On the defensive side, we can expect mid-size businesses to mature in their cybersecurity approach. Cyber risk is increasingly a board-level issue, not just an IT problem. By 2029, more mid-market firms will have adopted formal cybersecurity frameworks (such as NIST CSF or CIS Controls) and possibly even employ dedicated cybersecurity officers or virtual CISO services. Cybersecurity budgets are forecast to grow yearly as a percentage of IT spend, especially if regulators mandate minimum standards. Cyber insurance may become standard practice, potentially even required by business partners or investors as part of due diligence.

Importantly, collaboration and information-sharing will be key. Mid-size companies should leverage community resources – for example, participating in sector-based cyber threat exchanges or subscribing to threat intelligence feeds from the Canadian Centre for Cyber Security. Governments are also ramping up support; the federal government's Cyber Security Strategy envisions more outreach to help businesses strengthen their cyber resilience. We may see incentives or grants for cybersecurity improvements in the mid-market, given their importance to the economy and as suppliers to critical infrastructure

Cybersecurity budgets are forecast to grow yearly as a percentage of IT spend, especially if regulators mandate minimum standards.

Cybersecurity Comparison by Organization Size

Timeline	Key Focus Areas	Actions
Year 1	Foundation Building	• Implement MFA across all systems • Develop incident response plan • Deploy endpoint protection • Establish regular backups • Begin security awareness training
Years 2-3	Defense Enhancement	• Adopt zero trust architecture • Implement cloud security tools • Develop supplier security program • Enhance monitoring capabilities • Formalize security governance
Years 4-5	Optimization	• Deploy advanced threat detection • Implement security automation • Develop AI security capabilities • Establish threat hunting program • Create security innovation process

In summary, the period through 2029 will be challenging but manageable for mid-size organizations that stay proactive. Those who treat cybersecurity as a continuous business risk – akin to financial or operational risk – will fare best. This means keeping security on the leadership agenda, investing in people (training and talent) and technology, and rehearsing responses to incidents. It also means being adaptable: as new threats emerge (be it an IoT botnet or an AI-driven scam), being ready to assess the risk and implement safeguards. Mid-size companies that strike this balance – agility of a smaller firm combined with the strategic outlook on security of a larger enterprise – will not only withstand cyber attacks better but can even use strong cybersecurity as an enabler of trust and business growth.

The cybersecurity journey is ongoing. By learning from the past year's trends and preparing for those on the horizon, Canada's mid-size businesses can navigate the digital threat landscape with confidence.

About This Report

This comprehensive analysis draws on research from leading security organizations, government agencies, and industry surveys to provide mid-size Canadian businesses with actionable intelligence on the evolving cybersecurity landscape.

Key sources include:

- KPMG's Cybersecurity Research
- Canadian Centre for Cyber Security National Threat Assessment
- Statistics Canada Cyber Recovery Spending Report
- Proofpoint's 2024 State of Phish Report
- OpenText Cybersecurity's 2024 Ransomware Survey

Cybersecurity Resources for Mid-Size Organizations

- CyberSecure Canada Certification Program
- Canadian Centre for Cyber Security Publications
- Insurance Bureau of Canada: Cyber Insurance Resources
- NIST Cybersecurity Framework

For more information or to discuss your specific security challenges, contact us.

Citations

1. https://www.bnnbloomberg.ca
2. https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-2024-state-phish-report-67-canadian-employees-willingly-gamble
3. 2024 Cloud Security Report By Check Point https://engage.checkpoint.com/2024-cloud-security-report
4. https://www.insurancebusinessmag.com/ca/news/cyber/cyber-threats-dominate-concerns-for-canadian-businesses-508400.aspx
5. IBM. "Predictive Maintenance and AI: Reducing Downtime by 40%." 2023.
6. Gartner. "Cloud Resource Optimisation Strategies for Mid-Market Businesses." 2024.
7. VMware. "Energy Savings Through Virtualisation: A Case Study." 2023.
8. International Energy Agency. "IT Sector Energy Consumption and Green Opportunities." 2023.
9. UN Global E-Waste Monitor. "Trends in E-Waste and Recycling." 2019.
10. Deloitte. "Supply Chain Security: Rising Risks in 2024." 2024.
11. Citizen Lab, University of Toronto. "Ransomware Trends in Canadian Enterprises." 2023.
12. Accenture. "AI in IT Operations: Unlocking New Efficiencies." 2024.
13. Nielsen. "The Sustainability Premium: Consumer Trends and Business Impact." 2023
14. Verizon's 2024 Data Breach Investigations Report (DBIR).https://www.verizon.com/business/resources/reports/dbir/?msockid=2a424dbe071f610b2409593206356025

Let's shape your
IT future together

Schedule a Consultation:
Explore how F12 Infinite can help you achieve your IT objectives.

Request a Cyber Security Assessment:
Identify gaps and opportunities in your current defences.

Access Additional Resources:
Visit our website for more insights, tools, and expert advice.

F12.net™

Take the first step today.
Contact F12 Infinite to discover how we can help your organisation lead with confidence in 2025 and beyond.

Contact Us

For more information or to get started, please reach out to us using the details below:

1-866-F12-8782 | www.f12.net | info@f12.net

Office Locations

Toronto:
220 Markland Street, Unit A-2,
Markham, ON L6C 1T6
Tel: (416) 736-8386

Vancouver:
200 – 17577 56 Avenue,
Surrey, BC V3S 1C4
Tel: (604) 576-9522

Edmonton:
213555 156 Street NW,
Edmonton, AB T5V 1R9
Tel: (780) 413-8458

We look forward to partnering with you to secure your business and drive success

FIT1137-03-2025-V2