IBC
Insurance Bureau of Canada

The Canadian Cyber Insurance Market

October 2025

Executive Summary

In 2025, Canada's cyber insurance market has entered a phase of cautious stabilization. Insurers saw improved underwriting results after several turbulent years, and competition is growing alongside increased capacity (see figure 1). At the same time, cyber threats continue to evolve, with criminals leveraging artificial intelligence (AI) for more convincing, efficient, and widespread attacks, underscoring that vigilance remains paramount. While anticipated federal cyber security legislation has yet to be enacted, efforts continue through collaborative initiatives between the cyber insurance industry and governments to strengthen Canada's cyber resilience. Small and medium-sized enterprises (SMEs) remain significantly underinsured, highlighting a need for greater awareness and accessible coverage options. This report reviews key developments and trends in 2025, with a focus on market dynamics, the evolving risk landscape, regulatory progress, and SME cyber resilience.

This report is intended for **government officials, regulators, insurers, and business leaders** committed to strengthening Canada's cyber resilience. It highlights the urgent need for coordinated action across the public and private sectors to safeguard consumers, support businesses, and ensure the long-term stability of the cyber insurance market. The report also sets out key recommendations to better protect Canadians from growing online threats.

The report examines:

- **The cyber insurance market trends and industry outlook**
- **The evolving cyber risk landscape in Canada**
- **Legislative developments and the policy landscape**
- **The small and medium-sized enterprise cyber insurance gap**

Key Findings and Recommendations

The cyber insurance market trends and industry outlook

Rapid Market Growth: Cyber insurance written premiums surged from $18M in 2015 to approximately $650M in 2024, driven by rising demand across sectors.

Underwriting Losses & Hard Market: The ransomware epidemic (2019–2021) led to severe losses, with average combined loss ratios of 155%, impacting the cost and scope of coverage available.

Market Stabilization: By 2025, stricter underwriting and improved risk selection had led to profitability, with service ratios dropping to 49%. This has helped stabilize rates for well-managed risks.

Refined Underwriting Practices: Many insurers require baseline cyber controls (e.g., multi-factor authentication, backups, training), improving portfolio quality.

Increased Capacity & Maturity: Reinsurers have returned, enabling broader coverage and higher limits. New entrants and managing general agents (MGAs) are expanding offerings, which could signal a more predictable and sustainable market.

Healthier Competition: Organizations with strong cyber hygiene could secure better terms and discounts, reinforcing a positive feedback loop between risk management and pricing.

Ongoing Uncertainty: Despite improvements, systemic cyber events remain a threat. Competitive pressures could lead to imprudent underwriting if not carefully managed.

New Products & Innovation: Personal cyber insurance is emerging, covering identity theft, ransomware, and reputational harm. Insurance-linked securities (ILS) are expanding capital access and resilience against catastrophic events.

The Evolving Cyber Risk Landscape in Canada

AI-Driven Threats

- Generative AI enables convincing phishing and deepfakes, fueling harder-to-detect social engineering attacks.
- AI-enhanced malware is emerging, capable of adapting to victims' defenses.
- Ransomware is increasingly automated and may soon use AI to target data more strategically.
- AI-as-a-service lowers barriers, allowing low-skilled attackers to launch sophisticated campaigns.

Escalating Ransomware Risk

- Ransomware remains the top driver of large cyber claims in Canada, growing in frequency, complexity and cost.
- In 2023, global incidents rose 74%, ransom payments topped US$1B, and Canadian incidents grew 26% annually since 2021, with average payments of $1.13M.
- Professionalized "Ransomware-as-a-Service" models now use double and triple extortion tactics.
- Mid-sized firms, municipalities, hospitals, and SMEs are increasingly targeted due to weaker defenses.

Other Persistent Threats

- Business email compromise, supply chain breaches, and critical infrastructure attacks continue to rise, often amplified by AI tools.
- Attackers use encrypted channels and off-hours timing; global dwell time fell to 10 days in 2023, still enough to cause major harm.

Implications for Insurers

- Claims are rising in frequency and severity.
- The evolving threat landscape is testing policy language and driving demand for more tailored coverage and proactive risk services.

Legislative Developments and the Policy Landscape

- **Regulatory Progress Has Been Uneven**
  Bill C-26, aimed at modernizing Canada's cyber security framework for critical infrastructure, advanced through several legislative stages in 2024 but was not enacted into law after the federal government was prorogued in January of 2025. Its successor, Bill C-8, was introduced later in 2025 but remains pending.
- **Privacy Legislation is Also Stalled**
  Bill C-27, which would have modernized privacy legislation and established a framework for AI regulation, died on the order paper, leaving Canada's data protection framework outdated and fragmented.
- **Canada Lacks a National Cyber Framework for Critical Infrastructure**
  This legislative gap leaves essential sectors – like energy, telecom, and finance – without consistent, enforceable cyber standards, increasing systemic risk.
- **Interim Strategy Focuses on Collaboration**
  The federal government's renewed National Cyber Security Strategy emphasizes partnerships with the Canadian Cyber Defence Collective (CCDC) facilitating cross-sector coordination and information sharing.

Recommendations for policymakers to reduce Canada's risk of cyber threats:

- **Create a National Cyber Framework for Critical Infrastructure**
  Introduce a National Cyber Resilience Framework for Critical Infrastructure, requiring CNI operators (as defined by federal government) to meet minimum cybersecurity standards, with tailored implementation guidance by sector.
- **Support Cross-Sector Collaboration**
  Expand initiatives like the Canadian Cyber Defence Collective to improve information sharing, incident response, and systemic risk awareness.
- **Align with International Standards**
  Harmonize Canada's cyber regulations with global frameworks to improve resilience and attract international insurance capacity.
- **Explore a Cyber Catastrophe Facility**
  Consider a government-backed insurance mechanism to protect against large-scale cyber events, similar to terrorism risk pools.

The SME Cyber Insurance Gap

- **SMEs are Highly Vulnerable Yet Underinsured**
  Despite facing growing cyber threats, only 12% of Canadian small businesses have standalone cyber insurance coverage.
- **Low Awareness and Misconceptions Persist**
  Many SME owners underestimate their cyber risk or mistakenly believe general business insurance or IT providers offer sufficient protection.
- **Products Historically Misaligned**
  Traditional cyber insurance offerings did not often match SME needs, with coverage limits and features geared toward larger firms.
- **Cyber Readiness is Uneven**
  Many SMEs lack dedicated IT staff and basic protections, making underwriting and risk assessment more difficult.
- **Market Conditions are Improving**
  As pricing stabilizes in 2024–2025, insurers are beginning to offer more tailored, affordable, and modular coverage options for SMEs.

Recommendations for a healthier SME cyber risk landscape

- **Expand Education and Outreach**
  Governments should work with insurers, brokers, and industry associations to help SMEs better understand cyber risk as a core business threat and clarify what cyber insurance can cover.
- **Create a Cyber Readiness Incentive Program**
  The federal government should introduce targeted financial supports (e.g., tax credits, grants, or cost-sharing) to help SMEs invest in essential cybersecurity tools, training, and risk-management practices.

Market Trends and Industry Outlook

Market Trends and Industry Outlook

Market Growth and Stabilization

Cyber insurance has firmly established itself as a key component of the Canadian commercial insurance landscape. The market's growth has been dramatic as organizations large and small seek financial protection against cyber incidents. Written premiums have climbed from about $18 million in 2015 to approximately $650 million in 2024.[1,2] However, this rapid growth was accompanied by equally rapid increases in claims frequency and severity, especially during the ransomware epidemic[3,4] of 2019–2021. Insurers faced unprecedented losses; between 2019 and 2023, Canadian cyber insurers' combined loss ratios averaged approximately 155%, indicating severe underwriting losses.[5] This culminated in a hard market by 2021–2022, marked by rising premiums, tighter coverage limits, and some insurers pulling back capacity.

Figure 1.

Financial results under IFRS 4[6]	Direct Premiums ($Millions)	Claims Costs ($Millions)	Combined Loss Ratio[7]
2019	119	118	130.9%
2020	162	600	402.1%
2021	279	322	146.6%
2022[8]	472	(135)	3.3%
Financial results under IFRS 17	**Insurance Revenue**	**Insurance Service Expenses**	**Insurance Service Ratio[9]**
2023	550	458	94%
2024	650	252	49%

1 IBC, 2024.
2 International Financial Reporting Standard (IFRS) 17, implemented on January 1, 2023, has changed some of the fundamental concepts and presentation of financial indicators. As a result, these two sets of KPIs are similar but not exactly comparable.
3 Axios, May 17, 2021. The new digital extortion.
4 Marsh, Ransomware: A persistent challenge in cyber insurance claims.
5 IBC, 2024.
6 Accounting system for insurance contracts before January 1, 2023.
7 This ratio measures the profitability of underwriting while taking into account the claims ratio (claims costs and adjustment expenses) and expense ratio (underwriting expenses that are directly attributable to insurance contracts).
8 In 2022, cyber insurers in Canada reserved more funds than they needed to cover claims due to uncertain macroeconomic conditions, resulting in negative aggregated claims costs, which skewed the loss ratio for this line of business.
9 This ratio is a key profitability measure of insurance service result and represents the relationship between claims costs and insurance service result that are directly attributable to insurance contracts and insurance revenue.

Market Trends and Industry Outlook

Improved Loss Ratios

By 2025, there were clear signs that this cycle was tempering. Stricter underwriting and risk selection, coupled with rate increases in prior years, had materially improved loss ratios.[10] Notably, 2024 results show an insurance service ratio[11] of 94%, meaning insurers paid out roughly $0.94 in claims/expenses for each $1 of premium – a much-improved result compared to the deep losses of 2020–2021.[12] In 2025, the service ratio was even better, at 49%. Although accounting changes resulting from the implementation of IFRS 17 affect year-over-year comparability,[13] there is general consensus that cyber insurance in Canada has returned to underwriting profitability. This recovery has boosted confidence among insurers and reinsurers. Insurer profitability, though tentative, has led to a stabilization in market conditions. In some cases, renewal rates levelled out or decreased for well-managed risks, a stark contrast to the double-digit rate increases seen a few years ago.

Refined Underwriting Practices

A key factor in stabilization was the refinement of underwriting standards. Some insurers adjusted coverage terms to better manage emerging risks; for example, introducing sub-limits or exclusions for certain high-severity perils such as state-sponsored attacks or widespread outages. Many underwriters now commonly require policyholders to maintain baseline cyber security controls (e.g., multi-factor authentication, regular data backups and, employee training) as a condition of coverage. These measures have filtered out poorly protected risks and reduced avoidable losses. As a result of this more disciplined approach, competition has improved after the corrective phase. Where a few years ago some insurers were limiting cyber coverage, now new entrants in the market are expanding offerings, seeing opportunity in a line of business that is becoming more actuarially predictable.

Increased Capacity and Market Maturity

The influx of capacity is evident through higher available limits and a broader appetite for risk. Reinsurers, in particular, have regained an appetite for cyber insurance after observing better loss performance. This has allowed primary insurers to obtain reinsurance more easily and at a more reasonable cost, which, in turn, lets them write more business. Some specialist insurers and MGAs are also scaling up their Canadian cyber portfolios. Overall, these developments point to a maturing market: insurers and investors are treating cyber risk as a manageable, insurable peril, albeit one that requires constant attention.

Healthier Competition

As capacity returned to the market, clients saw some relief. Where coverage limits had been slashed during the hard market (with many companies only able to buy $5 million to $10 million insurance coverage limits), now higher limits are available and at more stable pricing. In some instances, organizations with strong cyber security measures are even securing premium discounts or more favourable terms as insurers compete for better risks. This trend of incentivizing good cyber hygiene illustrates a positive feedback loop: it encourages insureds to invest in security (to get better rates), which, in turn, should reduce losses for insurers. The consensus for 2025 is that the market is "right-sizing" – pricing is more aligned to risk, coverage is more clearly defined, and capacity is growing at a sustainable pace.

10 The loss ratio is the ratio of total losses paid out in claims plus adjustment expenses divided by the total earned premiums. Usually expressed as a percentage.

11 This ratio is a key profitability measure of insurance service result and represents the relationship between claims costs and expenses that are directly attributable to insurance contracts and insurance revenue. A ratio over 100% generally indicates a loss in insurance service result.

12 IBC, 2024.

13 A new international financial reporting standard on accounting for insurance contracts (IFRS 17), came into effect on January 1, 2023. The new global standard replaces IFRS 4, which had been in place since 2004.

Market Trends and Industry Outlook

Ongoing Uncertainties

Despite these positive signs, insurers remain cautious. The future profitability of cyber insurance is still uncertain. Cyber risk is dynamic, and a single large-scale event (for instance, a massive cloud service breach or a wide-reaching malware outbreak) could produce correlated losses that challenge the industry's capital. Moreover, as competition increases, there is pressure to loosen underwriting or cut prices, which if done imprudently, could sow the seeds of another difficult cycle. Thus, the prevailing sentiment is guarded optimism: the industry is on firmer footing and more experienced now, but prudent risk management and innovation (in both underwriting and risk mitigation) are crucial to maintaining momentum.

New Products and Offerings

In tandem with market stabilization, insurers have been diversifying their cyber offerings. One notable trend is the growth of personal cyber insurance. Traditionally, cyber coverage was almost exclusively a commercial product, but recent high-profile cyber incidents (such as identity thefts, financial account hacks, and cyber extortion scams) have driven demand for personal coverage. In response, insurers in Canada have begun introducing personal cyber policies or endorsements. These typically cover individuals and families for expenses related to restoration after identity theft, ransomware payments (e.g., if a home computer is locked), data recovery, and even cyber bullying or reputational damage in some packages. While still a nascent market, personal cyber insurance is bringing cyber risk transfer to the consumer level, and early uptake suggests a growing awareness among individuals of cyber threats beyond the corporate world. This also represents a new growth avenue for insurers, leveraging their cyber expertise in the retail insurance space.

Risk Transfer Innovations

Another innovation bolstering the market is the use of insurance-linked securities (ILS) and other alternative risk transfer mechanisms for cyber insurance. The cyber catastrophe bond sponsored by Beazley, an insurer, in early 2023 is a prime example, marking the first time that capital markets directly assumed cyber catastrophe risk.[14] The bond provides indemnity protection for extreme, systemic cyber events (those causing over $300 million in losses) and is tradable, expanding the pool of risk-bearing capital beyond traditional reinsurers. Its successful placement demonstrated investor confidence in well-underwritten cyber portfolios and a belief that catastrophic cyber risk can be quantified and modelled. Building on this precedent, 2024 saw six cyber catastrophic bond issuances across four sponsors, totalling $785 million. Industry experts anticipate additional ILS transactions or parametric coverage[15] in the coming years, which would further increase market capacity and resilience against mega-cyber events. These developments are indicative of a more robust, innovative market that is proactively seeking ways to handle tail risk scenarios.[16]

The Canadian cyber insurance market in 2025 is more stable and mature than in prior years. Insurers have adapted to the challenge of a high-risk environment through better underwriting and risk management and are now cautiously expanding their footprint. Clients are benefitting from this stabilization through improved availability of coverage. Yet, insurers and insureds are aware that the landscape can shift quickly. The next section explores how the cyber risk landscape itself is evolving, which, in turn, will influence future market dynamics.

14 Beazley, January 9, 2023. Beazley launches market's first cyber catastrophe bond.

15 Insurance that pays out based on a predetermined parameter or trigger, rather than assessed losses.

16 Tail risk refers to the possibility of rare, extreme events that lie at the far ends (or "tails") of a probability distribution - especially those that result in significant financial loss.

The Evolving Cyber Risk Landscape in Canada

The Evolving Cyber Risk Landscape in Canada

Cyber threats in 2025 continued to grow in sophistication, keeping pressure on insurers and organizations to stay ahead of attackers. Two major trends defined the 2025 risk landscape: the rise of AI-enabled attack techniques and the persistent threat of ransomware that adapts to countermeasures. Understanding these evolving threats is critical for insurers (to refine coverage and modelling) and for businesses (to bolster defences) because these threats directly impact claim frequency and severity.

AI-Driven Threats and New Attack Vectors

One of the most significant developments in the cyber threat landscape is the weaponization of AI by malicious actors. Over the past year, threat groups have increasingly leveraged generative AI tools to conduct more convincing and scalable social engineering attacks. For example, AI-powered phishing campaigns are now commonplace – attackers use large language models to generate highly persuasive, context-specific emails that mimic an individual's writing style and tone, making phishing lures harder to distinguish from legitimate communications.[17] These AI-generated messages are often grammatically flawless and tailored to the target, improving their success rate. In practice, this means even well-trained employees might be fooled, leading to more breaches of businesses' cyber systems via stolen credentials or malicious links.

Another alarming vector is the use of deepfake technology. Generative AI can create realistic audio and video imitations of trusted people. Cyber criminals have begun exploiting this in schemes such as business email compromises and executive impersonations. For instance, a fraudster might use an AI-generated voice clip of a CEO or use a deepfake video in a phishing email to add authenticity to convince an employee to initiate a wire transfer. The Canadian Centre for Cyber Security (Cyber Centre) warns "generative AI tools enable cyber threat actors to create realistic audio and visual content impersonating trusted individuals (i.e., deepfakes) helping to establish legitimacy with and persuade targets."[18] Such deepfake-enabled social engineering can defeat traditional verification controls and has already resulted in cyber incidents internationally.

Beyond phishing, AI is also being used to enhance malware. Security researchers note the emergence of malware that can autonomously adapt or evade detection. While still in early stages, attackers are also experimenting with AI algorithms that could allow malicious code to quickly change its behaviour to avoid antivirus software, or intelligently select targets within a network once inside. Likewise, AI can assist attackers in discovering vulnerabilities (by rapidly scanning code for flaws), potentially speeding up zero-day exploit development.[19] An example of this trend is the concept of "adaptive ransomware," which is ransomware that could eventually use AI to dynamically adjust its encryption methods or the data it targets based on a victim's backups or security responses – essentially optimizing the attack for maximum damage. Though current ransomware operations are not fully AI-driven, they are increasingly automated and sophisticated, foreshadowing this possibility.

These AI-driven threats elevate the risk landscape by making attacks more convincing, efficient, and widespread. They reduce the cost and skill barrier for attackers (even low-level cyber criminals can use AI-as-a-service tools to improve their scams) and increase the burden on defenders and insurers. For insurers, the rise of AI-enhanced attacks could translate to higher claim frequencies (because more successful phishing leads to more breaches) and potentially larger losses (if deepfake scams lead to high-value fraudulent transfers, for example). This underscores the need for continuous updates to underwriting questionnaires, such as those that assess how clients verify payments or train staff against AI-based phishing.

17 National Cyber Threat Assessment 2025–2026," Canadian Centre for Cyber Security.
18 IBID.
19 Zero-day exploit development refers to the process of discovering and creating tools or techniques that take advantage of previously unknown vulnerabilities in software, hardware, or firmware - before the vendor or public is aware of them.

The Evolving Cyber Risk Landscape in Canada

Ransomware and Evolving Threat Actors

While new AI-enabled attacks capture headlines, traditional cyber threats such as like ransomware continue to dominate the risk landscape and are evolving in tandem with defences. Ransomware remains the number one cyber crime threat facing Canadian organizations and critical infrastructure. Cyber insurers cite ransomware as the primary driver of large claims in recent years, and 2025 statistics reinforce that the threat is not abating.

The Cyber Centre identifies several alarming statistics in its "National Cyber Threat Assessment 2025–2026." According to Canadian cyber security authorities, "ransomware attacks have increased in scope, frequency and complexity," since 2020[20] (and 2023 was a record-breaking year globally for ransomware activity. The Cyber Centre cites one estimate that showed a 74% year-over-year increase in ransomware incidents worldwide in 2023, with total known ransom payments reaching approximately $1.368 billion – the highest on record.[21] In Canada, ransomware incidents reported to the Canadian Cyber Centre have grown by an average of 26% annually since 2021.[22] The average ransom paid by Canadian victims in 2023 was $1.13 million, an increase by almost 150% from two years prior.[23] These figures likely underestimate the true scope of ransoms paid, since many events go unreported.

Criminal ransomware enterprises have become highly professionalized and adaptive. Many operate on a Ransomware-as-a-Service model, with core developers leasing out ransomware kits to affiliates. This expands their reach while continuously improving the malware. As organizations improve their data backups and incident response procedures, ransomware groups adjust tactics; for example, they perform double extortion (stealing data before encrypting it to threaten leaks) and even triple extortion (attacking customers or partners of the initial victim) to increase the pressure to pay. They also target critical data and systems to inflict maximum business interruption.

The Canadian Cyber Centre notes that ransomware actors "constantly refine their tactics to maximize profits".[24] In effect, ransomware operations are becoming more agile and resilient to law enforcement action and defensive measures. A temporary dip in ransomware activity observed in 2022 (attributed to successful law enforcement takedowns of certain gangs) was followed by a resurgence in 2023, indicating that new groups or existing ones reconstituted quickly to fill the void.

We also see an expansion of the target scope. Initially, ransomware criminals focused on large enterprises and institutions (for big payouts), but many have since turned their attention to mid-sized and smaller businesses, which typically have weaker security. A number of these victims were resource-strapped entities, including municipalities, hospitals and SMEs. The implication is that no organization is "too small" to tempt an attacker, especially if they are part of a larger supply chain or have insurance that might pay out. This diversification of victims means a wider spread of losses across the economy, and it challenges insurers to extend coverage and risk management support to sectors that historically paid less attention to their cyber security.

20 National Cyber Threat Assessment 2025-2026 - Canadian Centre for Cyber Security.
21 IBID.
22 IBID.
23 IBID.
24 IBID.

The Evolving Cyber Risk Landscape in Canada

Beyond ransomware, other threats persist. Business email compromise scams continue to cause significant financial losses and are increasingly enabled by the kinds of AI tools noted earlier (e.g., deepfake voices in phone-based fraud). Supply chain attacks, in which hackers compromise a software vendor or IT service provider to exploit its clients, remain a serious concern. Such attacks can impact many insureds at once, potentially leading to an accumulation of risk for insurers. Critical infrastructure attacks (sometimes by state-sponsored actors or hacktivists) are another concern; incidents such as pipeline or utility hacks could cause not just economic loss, but also safety risks. While these broader threats are not new, their methods evolve alongside corporate defences. Attackers are now frequently attempting to evade detection by "living off the land" (using legitimate administrative tools maliciously), using encrypted channels, or timing their attacks outside business hours. The dwell time (the time an attacker is in a network before detection) has thankfully been dropping. In 2023, there was a global median of 10 days in 2023, down from 16 days in 2022, as per cybersecurity reports – but even 10 days is ample time for a skilled intruder to escalate an attack.[25]

Implications for the Insurance Industry

The ever-shifting threat landscape means insurers must remain agile. Policy wording is constantly being tested by new claim scenarios (e.g., coverage for fraudulent funds transfer via deepfake voice may fall under crime insurance or cyber insurance, depending on the terms). Insurers are increasingly partnering with cyber security firms to provide value-added services, such as AI-based email filtering tools, threat intelligence feeds, or incident response retainers. These services can help insureds prevent or mitigate losses from more advanced threats.

Underwriters in 2025 are asking more detailed questions about how organizations are handling new risks. For example: *Do organizations have verification protocols to counter deepfake fraud? Are they training staff about AI-enabled phishing? Have they segmented networks to limit ransomware spread?* The answers may influence coverage and pricing.

Cyber threats in 2025 were marked by both continuity and change. Ransomware and social engineering remained the top risks, but new technologies, such as AI, have increasingly turbocharged them. This raises the bar for cyber security across all organizations. For the cyber insurance market, this underscores that while underwriting performance has improved recently, the risk environment remains challenging. The next section examines how Canada's legislative and policy landscape is addressing (or failing to address) these cyber risks, and what that means for stakeholders.

25 Google Cloud Blog. April 23, 2024. M-Trends 2024: Our View from the Frontlines.

Legislative Developments and the Policy Landscape

Legislative Developments and the Policy Landscape

Effective cyber security requires more than market forces; - it also depends on clear, enforceable regulatory frameworks. In Canada, regulatory progress on this front has been uneven. In 2024, hopes were high for the passage of Bill C-26: *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* (Bill C-26), which aimed to modernize Canada's cyber security regime by introducing mandatory standards and reporting obligations for critical infrastructure sectors such as telecommunications, energy, finance, and transportation. Modelled on international regimes including the U.S. *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) and the European Union's Network and Information Security Directive (NIS2 Directive), Bill C-26 would have required designated operators to implement cyber security programs, report incidents, and remediate known vulnerabilities under federal oversight.

Although Bill C-26 advanced through several stages and was amended in the Senate, it ultimately failed to receive royal assent following the prorogation of Parliament in January 2025. This left Canada starting 2025 without a national cyber security law for critical infrastructure, which some in the cybersecurity and insurance industry considered a significant regulatory void.

On June 18, 2025, the federal government revived these efforts through the introduction of Bill C-8: *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* (Bill C-8), which reintroduces Bill C-26. While its passage is still pending at the time of writing this report, Bill C-8 signals a renewed federal commitment to creating a cyber regulatory framework. However, until Bill C-8 is enacted the legislative gap persists, posing ongoing risk and uncertainty for critical infrastructure operators and the insurance industry.

Implications of the Ongoing Legislative Gap

Critical infrastructure risk

Without a clear regulatory framework, the cyber resilience of essential systems, such as power grids, pipelines, telecommunications, and financial services, is left reliant on company discretion and sector-specific rules, which can vary widely. This fragmented approach increases the risk of systemic failures. A major cyber incident affecting critical infrastructure could have cascading impacts.

Canada lagging behind its global peers

Other jurisdictions seem to have already moved ahead with comprehensive cyber laws. The United States has enacted mandatory incident reporting requirements under its CIRCIA, and the European Union's NIS2 Directive has introduced obligations across critical sectors. By contrast, Canada lacks a cross-sector cyber framework, potentially making Canadian systems more attractive targets, vulnerable to cyber threats, and complicating international collaborations. For global insurers, Canada's regulatory posture may translate into heightened caution when deploying capital.

Legislative Developments and the Policy Landscape

Government Strategy in the Interim

In the absence of legislation, the federal government has shifted focus to policy initiatives and partnerships. Canada's renewed National Cyber Security Strategy, *Securing Canada's Digital Future*, outlines federal priorities through 2027. It focuses on infrastructure protection, cyber crime prevention, and whole-of-society coordination.

A key initiative under the strategy is the Canadian Cyber Defence Collective (CCDC), a national collaboration platform that brings together government, infrastructure operators, cyber security firms, insurers, and academics. The CCDC aims to facilitate information sharing, coordinate incident response, and promote best practices. For the insurance industry, this kind of collaboration is vital for understanding emerging systemic risks and exploring solutions such as a potential government-backed cyber catastrophe backstop, similar to terrorism insurance models abroad.

Privacy Legislation Stalled

Cyber risk is closely intertwined with data protection. In parallel with Bill C-26, the federal government had also introduced Bill C-27: *Digital Charter Implementation Act, 2022* (Bill C-27), which proposed the introduction of the *Consumer Privacy Protection Act* and the *Artificial Intelligence and Data Act*. If enacted, it would have strengthened privacy rights, increased penalties for non-compliance, and added new obligations around data use and AI systems. However, Bill C-27 also died on the order paper following Parliament's prorogation and has not yet been reintroduced. As a result, privacy regulation in Canada remains fragmented, adding another layer of uncertainty for businesses and insurers managing cyber risk.

The section that follows explores how this evolving landscape impacts one of the most vulnerable groups: small and medium-sized enterprises, which typically lack the resources and regulatory clarity to manage cyber risk effectively.

The SME Cyber Insurance Gap: Challenges and Opportunities

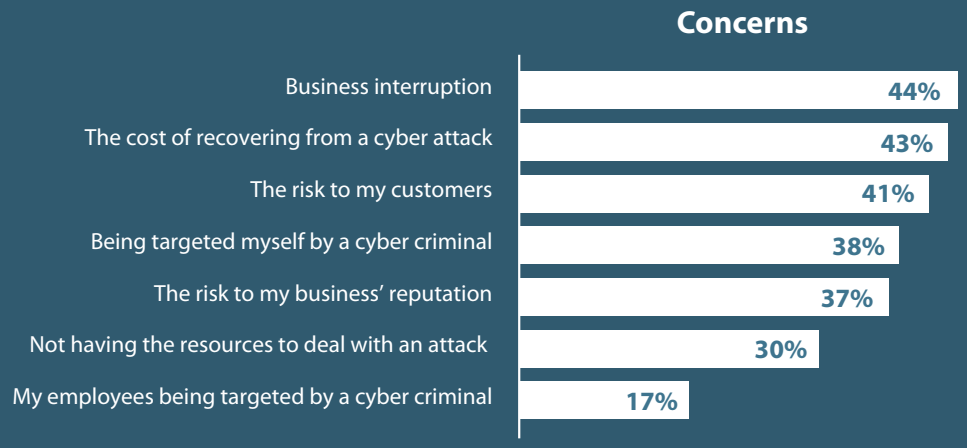
Attitudes Towards Cyber Risk

61% of SME respondents believe their business is too small to be targeted.

Cyber security is not a financial priority for 64% of SME respondents.

Only 12% of SME respondents have a standalone cyber insurance policy.

The top three cyber risk concerns for surveyed owners and decision makers at small and medium-sized businesses is business interruption, the cost of recovering from a cyber attack or data breach and the risk to their customers.



27% of respondents also say they are concerned about being sued due to a cyber attack.

Survey conducted by Angus Reid on behalf of Insurance Bureau of Canada from August 6 to 15, 2025. Full report available at www.cybersavvycanada.ca.

The SME Cyber Insurance Gap: Challenges and Opportunities

SMEs form the backbone of the Canadian economy, accounting for the majority of businesses in the country. Yet when it comes to cyber risk and insurance, SMEs are disproportionately vulnerable and underinsured. Many lack the resources of large corporations to invest in cyber security. In 2025, this segment continued to present a challenge: on the one hand, they faced growing cyber threats; on the other hand, their uptake of cyber insurance remained very low. This section examines the state of cyber risk for SMEs, why insurance uptake is so limited, and what efforts are underway (or are needed) to address this gap.

It is estimated that only about 12% of Canadian small businesses have standalone cyber insurance coverage.[26] Since the vast majority of Canadian businesses are SMEs, this statistic reflects the sparse adoption among smaller firms. This is not unique to Canada; other developed jurisdictions also see low take- up from the SME sector.[27] Even among medium-sized organizations that likely have some awareness of cyber risks, many have opted not to invest in a cyber insurance policy, especially if it is not contractually required by their business partners. This low uptake stands in stark contrast to the risk exposure; studies have shown that a significant percentage of cyber attacks (e.g., ransomware and, phishing) impact small businesses. In fact, cyber criminals often target SMEs precisely because they tend to have weaker defences and might be more willing to pay a smaller ransom quickly.

Challenges Facing SMEs:

Awareness and perception

A foundational issue is that many SME owners underestimate their cyber risk. There is a lingering myth that cyber attacks only happen to big corporations, or that a business with "nothing of value" won't be targeted. SMEs hold sensitive data (e.g., personal customer information, payment details) and can be entry points to larger networks, making them attractive targets. Awareness is improving slowly, especially as local news covers incidents of small businesses hit by data breaches or ransomware. However, a portion of SMEs underestimate their cyber risks while others may conflate it with general liability or assume their IT service provider handles all cyber issues. This gap in understanding means that even when insurance is available, it's not necessarily being sought. The insurance industry experts have identified education as a key to increasing SME uptake – business owners need to recognize cyber risk as a core business risk, akin to fire or theft.[28]

Cost and access

While awareness of cyber insurance among SMEs is growing, cost and accessibility remain common challenges. During the hard market period (2020–2022), premiums increased, and some small businesses found the pricing or deductibles unaffordable. The application process can also feel complex, particularly for businesses without dedicated IT support, as it often includes detailed questions about IT security practices. In some cases, coverage may be contingent on meeting specific baseline controls, such as implementing multi-factor authentication, which can require additional investment. As a result, some SMEs perceive cyber insurance as difficult to access due to both financial and operational hurdles. It's encouraging to note, however, that pricing has begun to stabilize in 2024–2025, creating greater opportunity for insurers to expand more tailored and accessible offerings for the SME segment.

26 Survey conducted by Angus Reid on behalf of Insurance Bureau of Canada from August 6 to 15, 2025.
27 For Australian and UK examples, see https://insurancecouncil.com.au/wp-content/uploads/2022/03/Cyber-Insurance_March2022-final.pdf? and https://www.gov.uk/government/publications/adoption-of-cyber-insurance-by-uk-small-and-medium-sized-enterprises?
28 Cornell University, September 29, 2023. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity.

The SME Cyber Insurance Gap: Challenges and Opportunities

Lack of tailored solutions

Historically, cyber insurance products were designed with medium-to-large businesses in mind, with coverage features and limits that may not have aligned with the unique needs of smaller firms or non-profit organizations. For example, a small retail business might only need $100,000 in coverage for data breach expenses and some business interruption. However, many insurers have offered higher coverage limits, such as $1 million, which may have come with a higher premium. Additionally, policy wordings sometimes include coverages that aren't relevant to small businesses (e.g., large crisis management costs) while leaving out important protections (e.g., coverage for lost income if an e-commerce site is disrupted). This mismatch has made it challenging for some SMEs to find a suitable fit. However, the landscape, is evolving. Insurers are increasingly offering micro-cyber insurance packages or flexible endorsements that can be added to a business owner's policy. These insurance packages are more tailored, modular options with lower limits and streamlined underwriting designed to provide "right-sized" coverage at more affordable price points for small businesses.

Cyber security readiness

Many SMEs are still in the process of building their cyber security capabilities, which can present challenges for both risk management and insurance. Smaller firms often operate without dedicated IT security staff. While many have some protections in place, such as antivirus software, basic firewalls, or data backups, implementation may vary depending on resources and awareness. From an underwriting perspective, this can make assessing and pricing risk more complex. In response, some insurers have introduced minimum security requirements (e.g., firewalls, antivirus and regular backups) to help ensure a baseline level of protection. SMEs that don't yet meet these requirements are often encouraged to enhance their cyber security and reapply, sometimes with support or guidance. As awareness grows and more accessible tools become available, improving cyber security readiness across the SME sector will support both resilience and insurability.

Consequences of Underinsurance

The low rate of cyber insurance among SMEs has several consequences. For individual businesses, it means a cyber incident can be financially devastating. Recovery costs from even a minor breach can easily reach tens or hundreds of thousands of dollars (requiring, for example, forensic IT work, data restoration, notification of affected customers and, legal fees), which many small firms would struggle to afford out-of-pocket. In the worst case, a serious cyber attack can force an SME out of business. At a macro level, widespread SME underinsurance means the Canadian economy will have to absorb those losses without the financial safety net that insurance provides. The challenge is doing so in a way that is sustainable for insurers and affordable for SMEs.

Efforts to Bridge the Gap

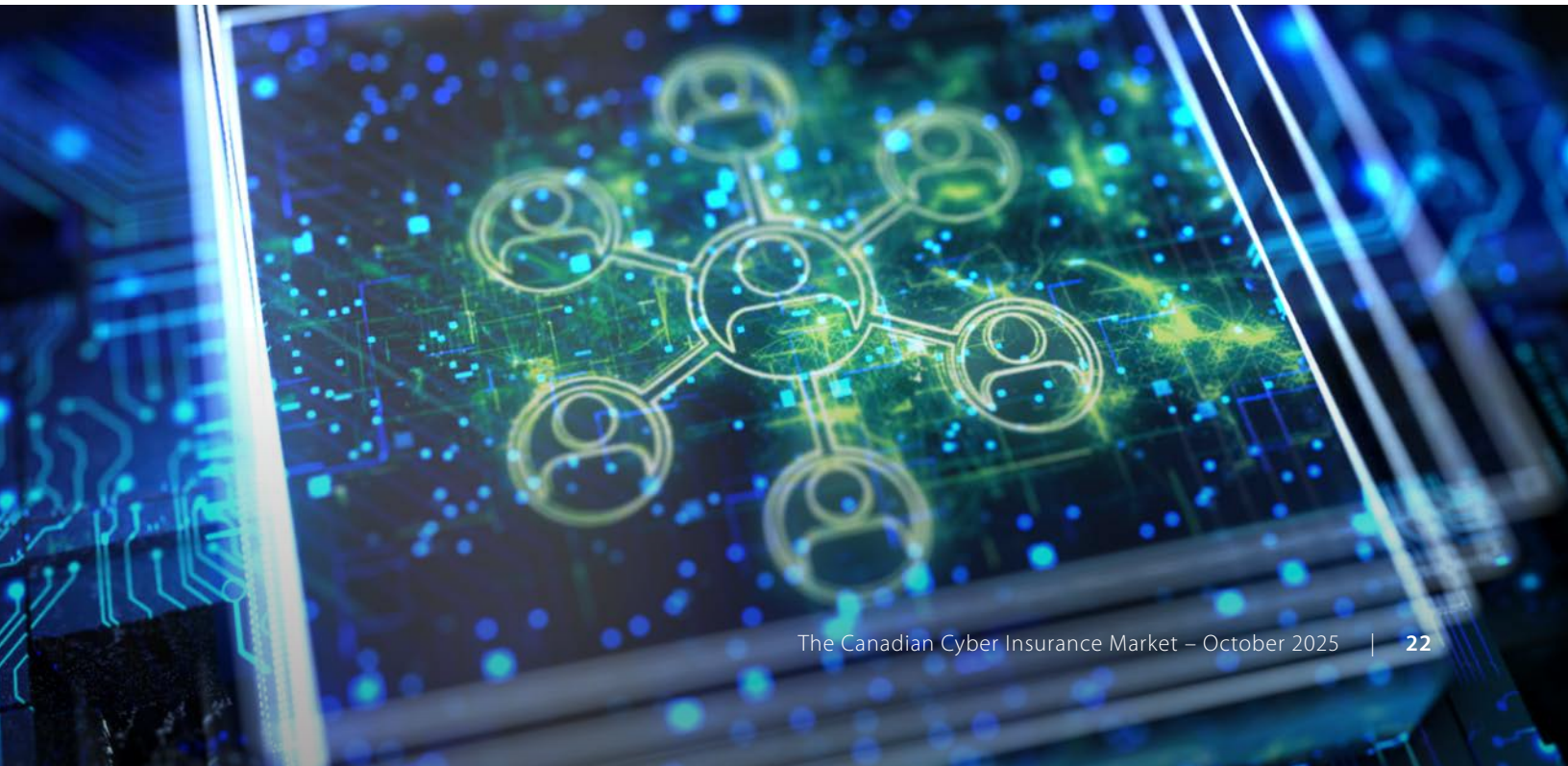
Both the insurance industry and Canadian governments have recognized the need to close the SME cyber coverage gap. Key initiatives include:

- **Education and awareness campaigns**
  The insurance industry and government are both playing an active role in improving cyber security awareness among SMEs. Insurance Bureau of Canada (IBC) runs an annual "Cyber Savvy" campaign, offering educational resources and a 10-question self-assessment tool to help small business owners understand their cyber risk profile and insurance readiness. By mirroring the types of questions insurers ask, the tool helps identify security gaps and encourages SMEs to make practical improvements. Insurers and brokers are also increasingly engaged in education efforts, -offering webinars, checklists, and advisory support to help SMEs understand their risk exposures and the steps they need to take to qualify for coverage. At the federal level, the "Get Cyber Safe" initiative provides simple, accessible guidance to promote cyber hygiene among businesses and individuals. Together, these efforts are helping to demystify cyber insurance, encourage better security practices, and support SMEs in taking meaningful steps toward resilience.

The SME Cyber Insurance Gap: Challenges and Opportunities

- **Product innovations for SMEs**
  Insurers are increasingly developing cyber insurance products tailored to the needs of small businesses. Many are offering cyber endorsements that can be added to existing general liability or property policies, providing basic coverage. This bundling approach can encourage uptake, as it can be presented at the point of sale as part of a broader insurance package. In parallel, some providers are simplifying the application and underwriting processes, using external data sources to assess risk or offering shorter, more accessible forms. These solutions often include value-added services such as breach response hotlines, which can be vital for businesses without in-house IT support. By making coverage easier to understand, more affordable, and integrated into existing policies, these innovations are helping to lower barriers and increase interest in cyber insurance among SMEs.

In summary, SMEs remain the "weak link" in Canada's cyber resilience chain; they are, largely uninsured and at risk. However, 2025 is seeing concerted efforts to engage this sector. There is growing awareness that protecting SMEs is essential for the overall security of commerce and supply chains, and it represents a growth frontier for insurers. If loss ratios continue to improve and insurers can craft sustainable products for smaller risks, there may be a significant expansion of cyber insurance into the SME market in the coming years.



Conclusion

In 2025, Canada's cyber insurance market stands on firmer footing than it had in the past, having emerged from a period of volatility with stronger underwriting, more predictable loss trends, and a broader array of products. Stabilized pricing, renewed capacity, and growing public-private collaboration signal that the market is maturing into a sustainable line of business.[29]

Yet this progress coincides with intensifying cyber threats. The rise of AI-enabled attacks and increasingly complex ransomware operations posed new challenges, underscoring the need for continued innovation and vigilance.[30] While insurers have modelled large-scale cyber catastrophes and expanded tools, such as reinsurance and catastrophe bonds, to manage large-scale cyber events, real-world events could test these assumptions.[31]

On the policy front, Bill C-26 was not enacted by the previous government, leaving an important gap in Canada's national cyber security framework, particularly for critical infrastructure, However the introduction of Bill C-8 signals the federal government's renewed commitment to establishing mandatory standards and oversight. In the meantime, initiatives like the Canadian Cyber Defence Collective and the broader National Cyber Security Strategy represent meaningful progress in strengthening cross-sector coordination, enhancing threat response, and laying the groundwork for a more resilient digital ecosystem.

Looking ahead, expanding cyber coverage to underserved segments, especially SMEs, remains an urgent priority. With only 12% of Canadian businesses insured, the protection gap presents both a vulnerability and a growth opportunity.[32] Closing it will require continued product innovation, targeted education, and, potentially, government-backed incentives to encourage adoption.

Canada's cyber insurance sector has entered a phase of cautious optimism. The foundation is stronger, but the threat landscape remains dynamic. Ongoing collaboration across industry, government, and businesses will be essential to building a cyber-resilient economy.

29 IBC, 2024.
30 Cyber Centre, 2024.
31 Insurance Business. Smith, J., 2023.
32 IBC, 2024.

Sources:

- **IBC (Insurance Bureau of Canada). (2024).** *Cyber Savvy Campaign Materials* – Tools aimed at improving SME cyber awareness and insurance preparedness, including a self-assessment tool.
- **IBC (Insurance Bureau of Canada). (2024).** *"The Canadian Cyber Insurance Market 2024."* – Key market statistics and insights on loss ratios, market growth, and emerging products.
- **Canadian Centre for Cyber Security. (2021).** *"Cyber Threat Bulletin: The Ransomware Threat in 2021."* – Statistics on ransomware incidents and their financial impact on Canadian organizations.
- **Canadian Centre for Cyber Security.** *"National Cyber Threat Assessment 2025-2026."*
- **Cyber Centre (Canadian Centre for Cyber Security).** *"National Cyber Threat Assessment 2023-2024."* – Analysis of threat trends, including AI-enabled attacks and ransomware statistics.
- **DiSabatino, A. (2024).** *"The rise and fall of cyber policy growth."* Canadian Underwriter.
- **Public Safety Canada. (2023).** *"Canada's National Cyber Security Strategy: 2023–2027."* – Federal strategy emphasizing public-private partnerships, including the Canadian Cyber Defence Collective (CCDC).
- **Araullo, K. (2024).** *"Beazley completes $140 million cyber catastrophe bond."* Insurance Business Magazine – Overview of the first cyber cat bond and its implications for market capacity.
- **Westman, R. (2025).** *"Canada's Draft Cybersecurity Legislation Must Be Resurrected."* Centre for International Governance Innovation – Discussion on Bill C-26's objectives and the impact of its failure.

ibc.ca