



IBC
Insurance Bureau
of Canada

The Canadian Cyber Insurance Market

**Insuring Cyber Risk
in an Interconnected
Economy**



October 2026

Executive Summary

This report finds that the Canadian cyber insurance market continues to mature as insurers' attention is increasingly focused on the severity of losses, the growing interconnectedness of digital systems and the persistent gap in cyber insurance adoption among small and medium-sized enterprises (SMEs).

This report presents three key findings:

1

Market conditions have stabilized. After a period of elevated claims and underwriting adjustments, insurer performance has improved significantly over the past few years. Industry data suggests the period of large loss ratios has eased, with recent results reflecting a return to more typical market conditions.

2

Individual claims continue to be large. Cyber incidents can be expensive and disruptive, often generating multiple costs at once, including business interruption, fraud losses, incident response expenses and privacy-related obligations. Although market performance has improved, large cyber events continue to influence the claims experience and underwriting outcomes.

3

Cyber risk is increasingly shaped by shared technology. Many organizations rely on the same cloud servers, software platforms and internet service providers. As a result, a disruption to a widely used technology can affect many organizations simultaneously, creating the potential for widespread losses.

In addition to providing financial protection, many cyber insurance policies give businesses access to specialized incident response services, including legal, forensic and recovery expertise.

Notably, many SMEs have not adopted cyber insurance. The results of an Insurance Bureau of Canada (IBC) survey indicate that in 2025, only 22% of SMEs carried cyber insurance, while only 12% had stand-alone cyber coverage.¹

Overall, the Canadian cyber insurance market is more stable than it was during the peak ransomware loss years between 2019 and 2021. The fundamental market challenge has changed from focusing on individual cyber incidents to how severe losses, shared technology dependencies and growing digital interconnectedness shape cyber risk across the economy.

The Growing Importance of Cyber Insurance

Cyber incidents generate immediate, significant financial and reputational consequences. A serious breach may result in business interruption, data recovery costs, legal and forensic expenses, privacy response obligations, fraud losses and

reputational damage. Canadian organizations are increasingly experiencing these consequences.^{2,3}

Cyber insurance's role extends beyond simply covering losses from an incident. Insurers are increasingly integrated into incident responses, providing timely access to forensic, legal and recovery expertise. This early engagement can help contain incidents faster and reduce their financial impact.^{4,5}

The early involvement of insurers is particularly important as cyber incidents are no longer limited to individual firms but can spread through broader networks, disrupting operations and affecting suppliers, customers and service providers. Insurer engagement is especially relevant in Canada, where SMEs play central roles in supply chains and local economies.⁶

Cyber insurance also promotes preparedness through underwriting requirements, such as ensuring that organizations implement cyber training for staff and regularly update their security software.

1 Insurance Bureau of Canada, [2025 Cyber Security Survey](#).

2 IBM Canada, ["IBM Report: Canadians' Data Security Under Increased Threat, While Breach Costs Surge."](#) IBM Newsroom Canada, July 30, 2025.

3 Maude St-Georges et al. ["Cyber Insurance Trends: 2026 Privacy Breach Insights – Part 5,"](#) McCarthy Tétrault, May 7, 2026,

4 IBID.

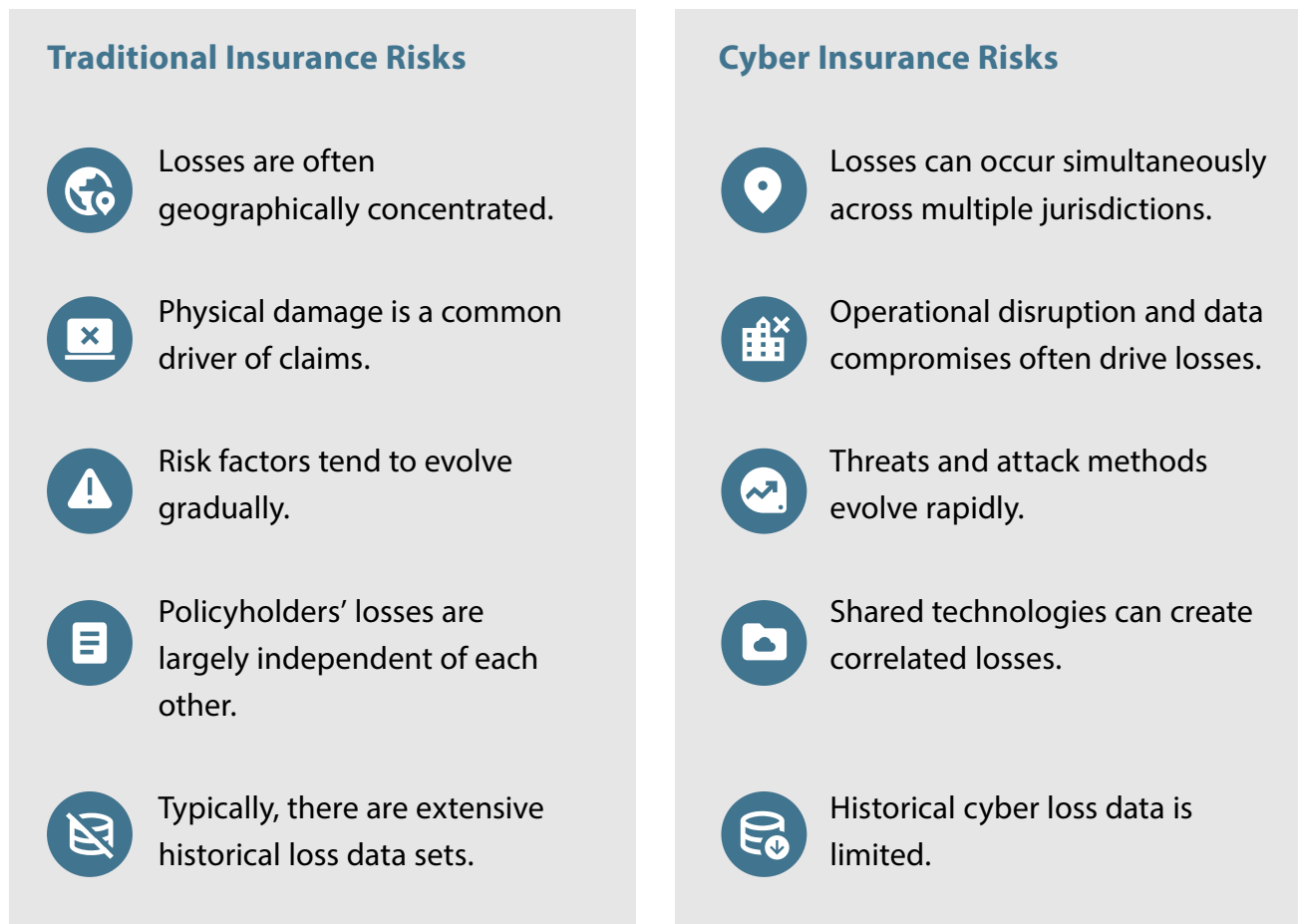
5 Coalition, ["Coalition 2025 Cyber Claims Report Finds Ransomware Stabilized but Remains Costly for Businesses,"](#) Coalition, May 7, 2025.

6 IBID.

What Makes Cyber Risk Different to Insure?

Though cyber insurance shares many characteristics with other forms of commercial insurance, it presents distinct challenges. Figure 1 contrasts traditional insurance risks to cyber insurance risks.

Figure 1. A comparison of traditional and cyber insurance risks

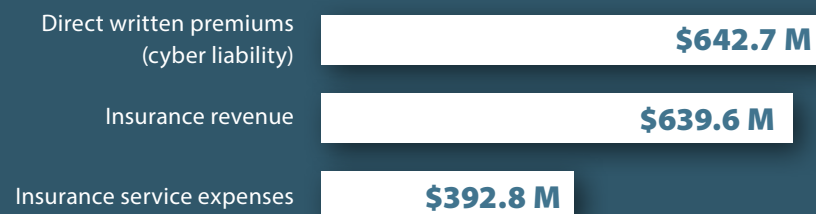


Another key distinction between traditional insurance and cyber insurance is risk observability and verifiability. In traditional property insurance, for example, many underwriting risk factors are tangible and relatively easy to assess, such as fire protection measures, building construction and occupancy. Many cyber controls, governance practices and third-party dependencies may change rapidly and may not be directly observable or independently verifiable at the point of underwriting.

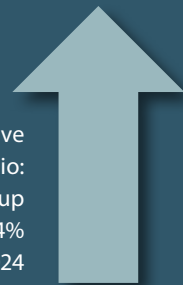
Market at a Glance

More Canadian businesses are purchasing cyber insurance, but recent results point to a more mature phase characterized by stable performance, persistent claims pressure and uneven coverage uptake.

Market Performance (2025)



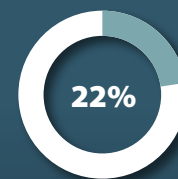
Comprehensive combined ratio: **72.6%** (2025), up from 57.4% in 2024



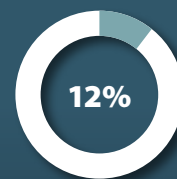
Risk Environment

- Average cost of a Canadian data breach: **\$7.11 million in 2026⁷**
- ↑ **\$6.98 million in 2025⁸**
- Businesses impacted by cyber incidents: **16% (2023)⁹**
- Fraud losses reported in Canada: **more than \$704 million (2025)¹⁰**

Coverage & Protection Gaps



SMEs with cyber insurance



SMEs with stand-alone cyber policies¹¹

⁷ IBM, 2026. *Cost of a Data Breach Report 2026*.

⁸ IBM, 2025. *IBM Cost of a Data Breach Report*.

⁹ Statistics Canada, 2024. *"Impact of Cybercrime on Canadian Businesses, 2023."*

¹⁰ CAFC.

¹¹ IBC 2025 Cyber Security Survey.

Market Performance

Market conditions remain stable, but recent results suggest a moderation in performance as claims pressure re-emerges.

As many companies pivoted to remote work due to the COVID-19 pandemic, cyber criminals took advantage of increased opportunities to attack systems, such as employees' greater reliance on mobile devices and less secure Wi-Fi networks. The high frequency of cyber breaches and ransomware attacks led to a sharp correction period with large underwriting losses.

The evidence now points to stabilization. Market conditions remain stronger than during the period of severe loss activity, but performance is no longer improving linearly.

The historical data illustrates the scale of the underwriting cycle and the subsequent correction in market performance.

Figure 2. IFRS 4 results¹³

Year	Direct Premiums (\$ millions)	Claims Costs (\$ millions)	Combined Loss Ratio
2018	92	42	79.0%
2019	136	118	130.9%
2020	224	600	402.1%
2021	329	322	146.6%
2022 ¹²	477	(135)	3.3%

Accounting system for insurance contracts before January 1, 2023.

¹² Claims reserves from cyber insurers in Canada proved larger than required and were released, resulting in negative aggregate claims costs.

¹³ 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.

Figure 3. IFRS 17 results¹⁴

Year	Insurance Revenue (\$ millions)	Insurance Service Expenses (\$ millions)	Comprehensive Combined Ratio
2023	550	458	93.6%
2024	650	252	49.2%
2025	639	392	66.0%

Source: MSA Research data shared with IBC, 2026.

Market results improved materially following the peak loss years, with 2025 reflecting stabilization of the market from pricing and loss perspective and normalized performance.

These results suggest that the market is neither hardening nor returning to the severe deterioration seen earlier in the peak loss years. Instead, 2025 reflects a moderation from unusually favourable conditions. In practical terms, the market has become more stable but remains sensitive to changes in loss severity.¹⁵

Broker reporting supports this interpretation. Competitive conditions persisted through 2025. Rate softening continued into early 2026, although the pace slowed as insurers placed greater emphasis on maintaining

portfolio stability. Market participants continue to report adequate capacity but also note increased underwriting scrutiny in sectors with elevated loss experience and concern related to systemic cyber risk.^{16,17}

Pricing, terms and capacity appear more closely linked to the strength of an organization's controls, governance and incident response capabilities.¹⁸

These trends point to a more mature, stable and selective market. The correction phase has largely restored underwriting discipline. Current market performance reflects continued attention to loss severity, underwriting discipline and exposure accumulation.

¹⁴ 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, financial results previous to 2023 are similar but not exactly comparable.

¹⁵ MSA Research, aggregated insurer claims data shared with the Insurance Bureau of Canada (IBC), 2026.

¹⁶ Willis Towers Watson, 2026. ["Cyber Risk: A Look Ahead to 2026."](#)

¹⁷ Gallagher, 2026. ["2026 Cyber Insurance Market Outlook."](#)

¹⁸ Willis Towers Watson, 2025. ["Insurance Marketplace Realities 2026: Cyber Risk."](#)

Market Structure

The Canadian cyber insurance market has become more specialized and risk-sensitive, with underwriting discipline and reinsurance support playing a central role in market conditions.

The cyber insurance market comprises traditional insurers, managing general agents, specialized cyber providers and reinsurers and brokers, which collectively provide capacity and expertise across a rapidly evolving risk landscape.

Cyber insurance policies remain broadly available to many organizations, particularly those that demonstrate strong cyber security practices. Brokers have reported policy prices are remaining flat and continued insurer appetite for well-managed risks, although several insurers have placed greater emphasis on portfolio stability and underwriting discipline.¹⁹

As a result, cyber insurance is increasingly differentiated by risk quality rather than broad market cycles. Insurers place significant weight on factors such as multi-factor authentication, endpoint detection, backup

procedures, incident response planning, governance practices and third-party risk management.

Reinsurance remains a core component of the market. Industry reporting indicates that cyber reinsurers continue to provide ample capacity, while maintaining a strong focus on accumulation risk, technology concentration and systemic cyber events. For example, Gallagher Re reported a capacity oversupply at January 2026 renewals, which improved pricing and structural terms for many buyers.²⁰

Taken together, these dynamics suggest that the Canadian cyber insurance market is competitive but not indiscriminate. Capacity is generally available, yet underwriting discipline, cyber security controls and exposure management continue to play central roles in how risk is assessed and priced.^{21,22}

¹⁹ Willis Towers Watson, 2026. [“Insurance Marketplace Realities 2026 Spring Update: Cyber Risk.”](#)

²⁰ Gallagher Re, 2026. [Gallagher Re Cyber Risk Adjusted Rating \(RAR\) Index: 2026 update.](#)

²¹ IBID.

²² Guy Carpenter, 2026. [“Cyber 2025—A Year in Review.”](#)

Claims and Insurability

Cyber losses are shaped by how often incidents occur and how costly they become when multiple loss drivers occur together.

Claims experience provides the clearest insight into what matters most in today's market. The key issue is how quickly losses can escalate when multiple cost drivers occur within a single event.

Current data points to a claims environment defined by rising event frequency, evolving loss composition and persistent exposure to low-frequency, high-severity events.

Public data aligns with this trend. IBM reports that the average cost of a Canadian data breach reached \$7.11 million in 2026.²³ Marsh indicates that privacy breaches remain the most frequently observed cyber threat, while ransomware continues to generate the largest and most complex losses.²⁴

Current claims experience reflects two interacting pressures:

1. High-frequency losses including fraud, privacy breaches and operational disruptions. These generate a steady volume of claims.
2. Low-frequency but high-severity events, particularly those involving ransomware or extended business interruption. These can drive disproportionate financial impacts.

Together, these two dynamics create a claims environment that can challenge profitability even under stable market conditions.

Social engineering is a central component of this environment. Fraud-related incidents represent a substantial share of claims volume and remain among the most consistent drivers of insured losses. These events exploit human and process vulnerabilities rather than technical system failures.²⁵

²³ IBM, 2025.

²⁴ Marsh, 2026. [US & Canada Cyber Claims 2025: Data Privacy Remains a Challenge While Ransomware Lingers.](#)

²⁵ Coalition, May 7, 2025. ["Coalition 2025 Cyber Claims Report Finds Ransomware Stabilized but Remains Costly for Businesses."](#)

Ransomware remains the dominant severity risk. Although the frequency of ransomware attacks has fluctuated over the years, the potential for large losses persists. Threat actors increasingly rely on data exfiltration and extortion, with amplified financial, regulatory and reputational consequences. The Canadian Centre for Cyber Security assesses ransomware as a persistent and evolving threat across all sectors.²⁶

These claims dynamics have direct implications for insurability. Underwriting increasingly reflects the presence and effectiveness of baseline cyber security controls. Insurers typically require multi-factor authentication, endpoint detection, secure backups, patching and incident response planning as standard expectations. As a result, insurability is increasingly linked to cyber security controls, governance practices and incident response capabilities rather than exposure alone.

Claims experience remains a key driver of cyber insurance market conditions, influencing pricing, underwriting decisions and coverage availability.

Case Study: Indigo Ransomware

Single cyber events can generate overlapping financial and operational losses across multiple parts of an organization.

In February 2023, Indigo Books & Music experienced a ransomware attack that disrupted both retail and digital operations. Systems supporting point-of-sale transactions, internal operations and e-commerce were affected, limiting the company's ability to conduct normal business activities. Public reporting indicates that stores were temporarily unable to process card payments and that online sales were unavailable for an extended period.^{27,28}

The incident also compromised employee data. Personal information related to current and former employees was accessed. But fortunately, customer payment data was not affected.²⁹

Indigo reported that the cyber attack contributed to losses of approximately \$50 million, reflecting both direct response and operational disruption costs.^{30,31}

²⁶ Canadian Centre for Cyber Security, 2026. "[Ransomware Threat Outlook 2025–2027](#)."

²⁷ CBC News, 2023. "[Indigo lost \\$50M last year, in large part due to February cyberattack](#)."

²⁸ Indigo Books & Music, 2023.

²⁹ CBC News, 2023. "[Indigo won't pay ransom for stolen employee data](#)."

³⁰ *IBID*.

³¹ Indigo Books & Music, 2023.

The importance of this case study lies not only in its scale, but in its illustration of modern cyber loss. Cyber incidents can simultaneously disrupt digital systems and physical operations, particularly where payments, retail activity and logistics depend on integrated technology platforms. Containment measures, including taking systems offline, may mitigate further compromise but can prolong business interruption.

Multiple loss components may arise from a single event, including business interruption, data compromise, incident response costs and reputational impact. The interaction of these factors is a key driver of severity in cyber insurance.

Digital Dependence and Systemic Cyber Risk

Shared digital dependencies mean cyber risk is not always independent across organizations. Disruptions affecting widely used technologies can impact multiple businesses simultaneously.

Cyber risk can no longer be understood solely at the level of individual organizations. Many firms that appear independent from an insurance perspective – by geography, sector or size – rely on the same cloud providers, software platforms, managed

service providers and digital infrastructure. As a result, a disruption affecting one widely used technology may affect numerous organizations simultaneously.

In cyber insurance, organizations separated by industry, location or size may nonetheless share common technology dependencies. This creates the potential for losses to emerge from a common source.

The increasing digitization of the economy has amplified these interconnections. Cloud computing, software-as-a-service platforms, managed service providers, payment systems and enterprise software have become integral to business operations. These technologies provide significant efficiency and security benefits but can also create concentrations of risk when large numbers of organizations rely on them.

The increasing digitization and connectivity of homes, vehicles, equipment and businesses are creating additional pathways through which a cyber event may result in physical damage, theft, bodily injury, business interruption, privacy loss or third-party liability. This can create complex interactions between dedicated cyber coverage and traditional property, casualty, crime, automobile and liability policies. Coverage outcomes will depend on the applicable policy language, including insuring agreements, definitions, exclusions, endorsements and causation provisions.

Recent incidents illustrate how these dependencies can produce widespread impacts.

CrowdStrike (2024)

A defective software update issued by cyber security provider CrowdStrike resulted in widespread global IT disruptions across airlines, financial institutions, health care organizations, retailers and government agencies. Although a malicious cyber attack did not cause the event, it demonstrated how disruption involving a widely used technology provider can have simultaneously affect thousands of organizations.

MOVEit (2023)

The exploitation of a vulnerability in MOVEit file-transfer software affected thousands of organizations globally through a commonly used technology platform. The incident demonstrated how a single software vulnerability can expose otherwise unrelated organizations.

SolarWinds (2020)

The SolarWinds compromise highlights how a supply-chain attack can propagate through trusted software providers, affecting large numbers of public and private-sector organizations through a common dependency.

These events did not originate within the affected organizations. Instead, they spread through shared technologies, service providers and digital infrastructure that connected numerous organizations.

The implications for insurers are significant. Traditional insurance relies, in part, on

diversification. Losses affecting one policyholder are often largely independent of the losses affecting another policyholder. Shared digital dependencies can weaken this assumption. When multiple insured organizations rely on the same technology platform, service provider or software product, a single disruption may simultaneously generate losses across numerous policyholders.

Vendor concentration is a key component of this risk. Many organizations depend on a relatively small number of providers for cloud computing, data storage, cyber security services, enterprise software and payment processing. While these providers often invest heavily in cyber security and operational resilience, their widespread adoption can increase the potential scale of disruption when an incident occurs.

Third-party dependencies further increase the complexity. Modern organizations operate within extensive digital eco-systems that include suppliers, contractors, managed service providers and outsourced technology partners. As a result, cyber incidents can cascade through business networks, creating operational and financial impacts beyond the originally affected organization.

These concerns are reflected in reinsurance markets. Industry reporting indicates that reinsurers continue to focus on accumulation risk, technology concentration and shared digital dependencies when evaluating cyber portfolios. While cyber insurance capacity remains broadly available, the potential for correlated losses remains a central consideration in portfolio construction and exposure management.

The Protection Gap: SMEs

The SME cyber protection gap creates exposures that can extend through supply chains and business networks.

The cyber protection gap among SMEs remains one of the clearest structural challenges in the Canadian market. An IBC survey found that only 22% of SMEs carried cyber insurance in 2025, and only 12% held stand-alone coverage. At the same time, less than half of SMEs reported having implemented basic cyber security measures.³²

This gap is not only a coverage issue. It also has implications for how cyber losses are absorbed across the broader economy. SMEs play a central role in Canada's economy as employers, service providers and participants in critical supply chains. When these firms are underprepared or uninsured, cyber incidents are less likely to be absorbed through structured mechanisms such as insurance.

Instead, firms, customers and business partners may bear the losses. These impacts are often less visible and less predictable, particularly when they propagate through supply chains or business relationships.

The protection gap reflects a combination of demand and supply factors. On the demand side, SMEs often face constraints related

to awareness, affordability and competing business priorities. On the supply side, underwriting requirements tied to baseline cyber security controls may create barriers to entry for firms with limited resources.

These factors can reinforce one another. Firms that lack the capacity to implement core controls may struggle to obtain coverage, which in turn may limit improvements in cyber security practices and preparedness. This creates a self-reinforcing cycle in which lower preparedness leads to lower coverage and greater vulnerability.

Cyber insurance plays a role in addressing this gap. Underwriting requirements can support improved baseline controls, while brokers and risk advisors can help translate cyber risk into practical business decisions.

The implications extend beyond individual firms. SMEs are often embedded in supply chains and local economies. Given the role of SMEs in supply chains and service delivery, cyber incidents affecting these firms can have impacts beyond the originating organization.

Cyber incidents affecting underinsured SMEs can create financial and operational impacts for suppliers, customers and business partners. Closing the cyber protection gap for

³² IBC, 2025.

SMEs is therefore not only about increasing insurance uptake. It is also about improving cyber preparedness and the ability of firms to absorb and recover from cyber losses.

Public Policy and Regulation

Cyber security policy and cyber insurance increasingly operate within the same risk environment. Developments in regulation, reporting, governance and international cooperation can influence how cyber risks are understood, managed and insured.

As cyber incidents become more economically significant, governments are devoting greater attention to cyber security, critical infrastructure protection, incident reporting and digital governance. While most of these initiatives are not directed at the insurance sector, they can influence the conditions under which cyber risks are measured, managed and transferred.

The following developments are particularly relevant to the cyber insurance market:

Strengthening Critical Infrastructure for Cyber Security

Canada continues to emphasize protecting critical infrastructure from cyber threats. The Federal Critical Cyber Systems Protection Act, which became law in June 2026 but still requires regulation to fully take effect, will strengthen cyber security requirements for designated operators in federally regulated sectors and improve incident reporting, governance and risk management practices.

This development is relevant to cyber insurance because organizations that support critical infrastructure often represent some of the most complex and potentially severe cyber risk exposures in the economy. Disruptions affecting telecommunications, energy, transportation or financial systems can generate consequences that extend beyond individual organizations and broadly affect economic activity.

From an insurance perspective, regulatory requirements related to cyber governance, incident management and cyber security controls can also influence underwriting expectations. As insurers increasingly emphasize the effectiveness of controls and organizational preparedness, regulatory standards may contribute to greater consistency in how cyber risks are managed and evaluated.

Incident Reporting and Cyber Risk Data

One of the longstanding challenges in cyber insurance is the availability of reliable incident and loss data. Compared with many traditional insurance lines, cyber insurance operates with a relatively short history of claims experience and less standardized loss information.

Recent policy initiatives in Canada and internationally have placed greater emphasis on mandatory incident reporting, disclosure requirements and information sharing. These efforts reflect a growing recognition that better data is essential to understanding cyber risk.

For insurers, improved incident reporting can provide greater insights into loss trends, threat activity and emerging exposures. Enhanced data may support underwriting, pricing, accumulation assessment and risk modelling over time.

This is particularly relevant in a market in which concerns increasingly extend beyond individual organizations to sources of correlated risk such as shared technologies and common service providers.

International Cooperation and the Ransomware Threat

Cyber risk is inherently cross-border. Threat actors operate internationally, ransomware campaigns target organizations across jurisdictions, and many digital services rely on globally interconnected infrastructure.

Canada participates in several international cyber security initiatives, including the Counter Ransomware Initiative, which seeks to strengthen cooperation among governments through information sharing, the disruption of cyber criminal activities and efforts to reduce ransomware-related financial flows.

Recently, Canada became a signatory to the United Nations Convention against Cybercrime, which contains measures aimed at preventing cyber crime through enhanced public awareness, stronger collaboration between the public and private sectors and targeted support for small businesses, acknowledging their importance to economic resilience and local communities.

The agreement aligns with the broader trend of Canada's growing participation in international cyber security frameworks and agreements, such as Five Eyes, that focus on strengthening cyber defence and cooperation.

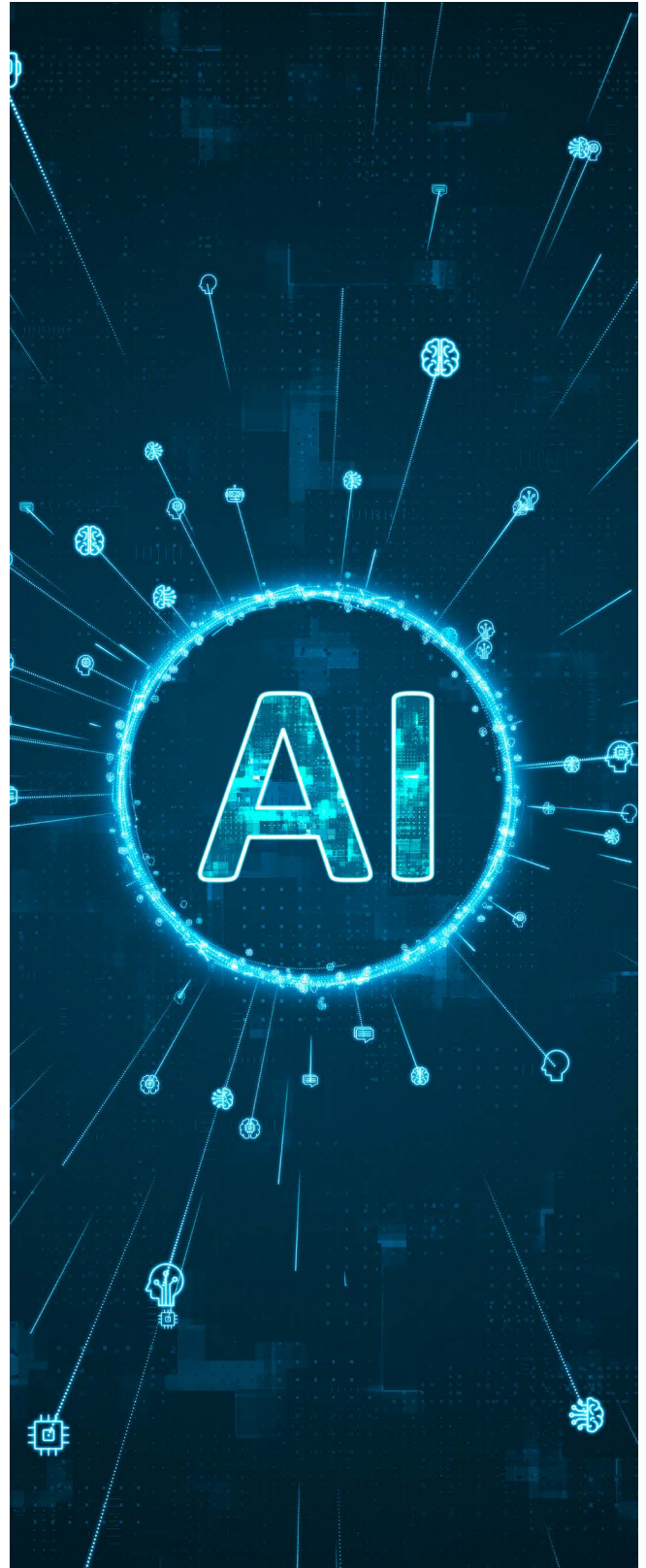
Artificial Intelligence and Emerging Risk

Artificial intelligence (AI) is becoming an increasingly important component of cyber security.

AI-enabled tools are being used to improve threat detection, monitoring and incident response. At the same time, these tools may increase the sophistication and scale of social engineering, phishing, impersonation and detecting security flaws.

The long-term implications of AI remain uncertain. However, it is increasingly being incorporated into broader discussions of cyber security policy, digital governance and organizational risk management.

For insurers, the primary significance lies in understanding how emerging technologies may influence cyber incidents. While AI may strengthen cyber defence capabilities, it can also alter the threat landscape in ways that are not yet fully understood.



Why It Matters for the Cyber Insurance Market

Public policy and cyber insurance increasingly operate within the same risk environment.

The most significant government policy developments are those that improve visibility into cyber incidents, strengthen cyber security practices, support information sharing and enhance the understanding of emerging risks. These factors help shape underwriting decisions, influence risk management expectations and contribute to a more informed assessment of cyber risk across the economy.

While government policy measures and insurance mechanisms serve different functions, both respond to the common challenges associated with cyber risks.

Key Implications

For governments: Digital dependence, persistent SME coverage gaps and the growing importance of systemic cyber risk are notable features of Canada's cyber risk landscape.

For the property and casualty insurance industry: Loss severity and accumulation risk remain central considerations despite stable market conditions. Underwriting discipline, loss severity and management risk continue to influence performance. Shared digital dependencies are a significant consideration for insurers.

For businesses: Cyber insurance and cyber security practices are increasingly interconnected. More and more, cyber insurance is linked to cyber security practices, operational preparedness and third-party risk management. As organizations depend more on digital systems, cyber risk expands beyond the boundaries of traditional IT functions.

Conclusion

The Canadian cyber insurance market has matured, but the risk environment has become more complex.

Market stabilization has largely been achieved following the severe loss experience between 2019 and 2021. Cyber risk is increasingly influenced by shared digital dependencies and concentrations of critical technology services.

As a result, the central issue facing the market is no longer whether cyber insurance can provide capacity and coverage. Today, the central issue is how insurers, businesses and policymakers understand and manage risks that may be severe, interconnected and difficult to diversify.



Selected Sources

- **Canadian Centre for Cyber Security.** Ransomware Threat Outlook 2025–2027. Government of Canada, 2026.
- **CBC News.** “Indigo lost \$50 million last year, in large part due to February cyberattack” June 28, 2023.
- **CBC News.** “Indigo won’t pay ransom for stolen employee data” March 1, 2023.
- **Coalition.** Cyber Claims Report. 2025.
- **Gallagher Re.** Cyber Market Outlook. 2026.
- **Gallagher Re.** Cyber Risk Adjusted Rating (RAR) Index: 2026 Update. January 2026.
- **Guy Carpenter.** Cyber 2025—A Year in Review. 2026.
- **IBM.** Cost of a Data Breach Report: Canada. 2025.
- **Indigo Books & Music Inc.** Public financial reporting and disclosures related to the February 2023 ransomware incident.
- **Insurance Bureau of Canada.** Cyber Security Survey. 2025.
- **Insurance Bureau of Canada.** The Canadian Cyber Insurance Market. October 2025.
- **McCarthy Tétrault.** Cyber Insurance Trends 2026: Privacy Breach Insights. 2026.
- **Marsh.** Cyber Claims 2025 Report. 2026.
- **MSA Research Inc.** Cyber insurance industry data analyzed by Insurance Bureau of Canada, 2026.
- **Statistics Canada.** Cyber security and cybercrime survey data, 2023.
- **Willis Towers Watson.** Cyber Risk: A Look Ahead to 2026. 2026.
- **Willis Towers Watson.** Insurance Marketplace Realities 2026 Spring Update – Cyber Risk. May 2026.
- **Willis Towers Watson.** Insurance Marketplace Realities 2026 – Cyber Risk. October 2025.

Note: Unless otherwise indicated, Canadian cyber insurance market statistics are based on Insurance Bureau of Canada analysis using MSA Research data for private property and casualty insurers operating in Canada.



ibc.ca

