



IBC
Insurance Bureau
of Canada

The Canadian Cyber Insurance Market 2024



Contents

04	Executive Summary
06	About Cyber Insurance
08	State of the Cyber Insurance Market
10	The Evolving Risk Landscape
12	New Approaches
14	Conclusion

Executive Summary

In recent years, the cyber insurance market in Canada market has shown significant growth potential as insurers adapted their offerings to meet the increasingly sophisticated cyber threats. This report offers an analysis of current cyber insurance coverage, highlights recent insurer financial results, and identifies emerging trends, threats, and opportunities within the cyber insurance landscape. Additionally, it details the role of industry, through Insurance Bureau of Canada (IBC), in fostering a cyber-resilient environment through resources for business owners and public education campaigns.

Key insights include the increased awareness of and demand for cyber insurance, driven by the rising frequency and severity of cyber-attacks, particularly ransomware. Insurers are responding by refining coverage scopes, adjusting underwriting standards, and incorporating exclusions to manage the rising claim costs, thereby contributing to market stabilization. This report also notes an increase in the sophistication of threats, such as business email compromises, with cybercriminals using advanced AI tools for more complex schemes. Furthermore, new products like personal cyber insurance and risk transfer mechanisms such as insurance-linked securities are bringing fresh offerings and increased capacity to the market. On a broader scale, the Government of Canada is implementing proactive measures to reduce the vulnerability of critical infrastructure and governmental bodies to cyber risks, reflecting a more comprehensive approach to national cybersecurity.






About Cyber Insurance

Cyber insurance is a specialty insurance product intended to help protect businesses from loss resulting from digital risks such as data confidentiality breaches, technology disruptions and cyber extortion.


What Is Typically Covered?

Cyber insurance can cover loss resulting from a range of cyber events, including:

-  **Data confidentiality breaches:** The loss of and/or unauthorized access to or disclosure of confidential or personal information.
-  **Technology disruptions:** A technology failure or denial-of-service attack.
-  **Cyber extortion:** A demand for payment under threat of causing harm to your data; for example, disabling your operations or compromising your confidential data.

This list is not exhaustive as cyber coverage can vary from insurer to insurer and is constantly evolving. Appropriate coverage should be customized to address the needs of a particular customer.

Cyber insurance can help a business cover a number of costs resulting from these events, including:

-  **Security breach remediation and notification expenses:** Notifying affected parties and mitigating potential harm from a privacy breach, such as providing credit monitoring to affected individuals.
-  **Forensic investigations expenses:** Hiring a firm to investigate the root cause and scope of the data breach.
-  **Legal costs and civil damages:** Paying for legal representation and possible damages related to a privacy or network security breach.
-  **Network systems and electronic data restoration expenses:** Restoring or recovering damaged or corrupted data caused by a breach, denial-of-service attack or ransomware.

Personal Cyber Insurance

Individuals are vulnerable to cyber risks as well as businesses. Personal cyber insurance is a relatively new offering that is gaining popularity. This product provides individuals with coverage against personal online security risks and financial losses due to cybercrime. Coverage options encompass a wide range of protections, including online shopping fraud, data breaches, identity theft, social engineering scams, and SIM swapping incidents. It also covers vulnerabilities linked to smart home devices and wearables, as well as ransomware or cyber extortion, and even cyberbullying and cyberstalking.

State of the Cyber Insurance Market

As cyber threats grow in frequency, magnitude, and sophistication, cyber insurance is emerging as an important component of the commercial insurance landscape. In 2015, insurers in Canada underwrote \$18 million in cyber premiums, a figure that has risen dramatically to over \$550 million in 2023. Despite this growth in market size, the frequency and severity of claims have escalated even more rapidly. Between 2019 and 2023, cyber insurance providers’ combined loss ratio averaged approximately 153%, meaning that for every dollar earned in premiums, insurers paid out \$1.53 in claims and operating expenses.

However, with historically elevated claims costs driven by the high frequency of cyber breaches and ransomware attacks, some insurers have adjusted their coverage scope, underwriting standards or

incorporated exclusions to better manage emerging cyber risks. Competition has returned to the market after a short, sharp correction, which was driven by improved loss ratios during the last couple of years. Improving conditions within the cyber market have encouraged more capacity to enter the market through renewed (re)insurer appetite, and new incumbents including managing general agents, and start-ups. This influx has improved policy limits and helped stabilize rate increases. Moreover, clients with robust security measures have sometimes secured discounts on premiums or obtained more favourable terms and conditions. While the future profitability of cyber insurance remains uncertain, these enhanced underwriting practices and a more refined perspective on cyber risk are expected to help stabilize the cyber insurance market in Canada.

Financial results under IFRS 4 ¹	Direct Premiums (\$Millions)	Claims Costs (\$Millions)	Combined Loss Ratio ²
2018	87	42	79.0%
2019	119	118	130.9%
2020	162	600	402.1%
2021	279	322	146.6%
2022 ³	472	(135)	3.3%
Financial results under IFRS 17 ⁴	Insurance Revenue	Insurance Service Expenses	Insurance Service Ratio ⁵
2023	550	458	83.4%

1 Accounting system for insurance contracts before January 1, 2023.

2 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).

3 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.

4 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.

5 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.



The Evolving Risk Landscape

The cyber risk landscape is continuously evolving. In 2023, the market witnessed:



Data breaches becoming costlier: The average cost of a data breach in Canada is steadily rising, reaching \$6.9 million⁶ in 2023, with widespread cyber crime and cyber insecurity ranking high among global industry leaders.⁷ The reinsurance industry remains wary of systemic risks, particularly prolonged cloud outages.



AI risks proliferate: AI introduces novel challenges in cyber security by enabling the automation of tasks involved in cyber attacks, rendering them more efficient and harder to detect. They can also be capable of adapting to cyber security defences in real time. Business email compromise and social engineering are growing more sophisticated and costly, aided by AI tools that enable more convincing scams.



Return of ransomware: Ransomware activity showed a resurgence in the first half of 2023, after a dip in 2022, reflecting new vulnerabilities cyber criminals are exploiting while refining their existing tactics.⁸



Awareness of Systemic Cyber Risk: The risk of systemic cyber events, wherein a single event affects multiple systems, organizations, or sectors simultaneously or sequentially, is a significant concern. Such events can propagate through industries due to interconnected digital systems and shared services, resulting in widespread economic repercussions. This has spurred a global dialogue on the merits of a cyber risk backstop.

International government leaders, insurance associations and regulators around the world are engaged in discussions about the potential need for a governmental backstop for catastrophic cyber events.⁹ The United States is currently reviewing the merits of a public facility to manage cyber risk.¹⁰ A governmental backstop would involve setting up a framework in which the government could provide financial support or guarantees to insurance companies facing overwhelming claims due to major interconnected cyber incidents. This would help stabilize the insurance market by guaranteeing that insurers can sustain operations and continue providing coverage, even in the face of severe systemic cyber events.

⁶ "Cost of a Data Breach Report 2023," IBM, [ibm.com/reports/data-breach](https://www.ibm.com/reports/data-breach).

⁷ "The Global Risks Report, 2018, World Economic Forum, (p.6), [weforum.org/publications/the-global-risks-report-2018](https://www.weforum.org/publications/the-global-risks-report-2018).

⁸ "Ransomware attacks setting record pace," Insurance Business, [insurancebusinessmag.com/ca/news/breaking-news/ransomware-attacks-setting-record-pace-464301.aspx](https://www.insurancebusinessmag.com/ca/news/breaking-news/ransomware-attacks-setting-record-pace-464301.aspx).

⁹ "A federal backstop for insuring against cyberattacks?" Brookings, [brookings.edu/articles/a-federal-backstop-for-insuring-against-cyberattacks](https://www.brookings.edu/articles/a-federal-backstop-for-insuring-against-cyberattacks).

¹⁰ "Potential Federal Insurance Response to Catastrophic Incidents," National Archives, Federal Register, The Daily Journal of the United States Government, [federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents](https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents).



New Approaches

In response to the increasing intensification of risks and attack vectors the insurance industry has adapted its approach through:

Advances in underwriting: Non-cyber markets are scrutinizing potential unintended silent cyber exposures (cyber risks are neither expressly covered nor excluded in an insurance policy), refining policy wordings to clarify coverage boundaries. Carriers are increasingly explicit in excluding cyber warfare and state-sponsored attacks, though their legal standing is yet to be fully tested. Loss modelling remains crucial for assessing the impact of cyber attacks across an entire portfolio. Advances in analytics empower cyber carriers and brokers, driving market growth and innovation.

Insurance-linked securities (ILS): ILS options such as cyber catastrophe bonds and industry loss warranties are emerging. These financial instruments provide insurers with a way to manage and mitigate large-scale cyber risks by transferring some of the risk to capital markets.¹¹

Developments in Canada

Bill C-26: This bill encompasses provisions to safeguard critical infrastructure and enhance the federal government’s capacity to respond to cyber threats.

Budget 2024 commitments: Canada’s 2024 Federal Budget includes significant cyber security investments aimed at enhancing the country’s defence and resilience. It includes improving security measures across government and key economic sectors to protect against increasing cyber threats.¹²

National cyber strategy renewal: Canada’s national cyber strategy is undergoing renewal, with a focus on bolstering national security, fostering economic prosperity and ensuring citizen safety in the digital era. This renewal entails updating policies, frameworks and actions to effectively address the evolving cyber threat landscape.¹³

The counter ransomware initiative (CRI): As the number of ransomware attacks escalate, the CRI aims to strengthen cyber security measures and awareness across its member states. In 2023, all 50 CRI member states took a unified stand against cyber threats by publicly rejecting the payment of ransoms to threat actors, reaching a consensus to refuse extortion demands.¹⁴

11 “Cyber ‘Catastrophe Bonds’ Move Step Closer to Hitting Public Debt Markets,” [bloomberg.com/news/articles/2023-11-12/cyber-catastrophe-bonds-move-step-closer-to-hitting-public-debt-markets](https://www.bloomberg.com/news/articles/2023-11-12/cyber-catastrophe-bonds-move-step-closer-to-hitting-public-debt-markets).

12 “2024 Federal Budget – Our Policy Experts’ Insights,” Canadian Chamber of Commerce, chamber.ca/news/2024-federal-budget-our-policy-experts-insights.

13 “Consulting on Canada’s Approach to Cyber Security,” Public Safety Canada, publicsafety.gc.ca/cnt/cnslttns/cnsltng-cnd-pprch-cbr-scr/index-en.aspx.

14 “International Counter Ransomware Initiative 2023 Joint Statement,” The White House, [whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement](https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/).



Conclusion

While market dynamics are showing signs of improvement, it's important to note that only about 5% of Canadian businesses currently have cyber insurance,¹⁵ highlighting a significant opportunity for market expansion. Traditionally, the primary constraint in cyber insurance growth was risk appetite, but with increased capital inflow and reinforced reinsurance capacity, the focus has shifted toward consumer education. There remains a notable gap in understanding the extent of cyber exposure for both businesses and households. To bridge this gap, the industry must collaborate with governments and regulators to emphasize the critical importance of cyber resilience. It is essential to educate consumers that cyber insurance serves as an effective risk transfer mechanism, but it is not a substitute for proactive cyber vigilance.

IBC's Role

IBC has been supporting businesses' efforts to increase their cyber resilience and understand risk mitigation measures, such as cyber insurance, through its annual Cyber Savvy public education campaign. It includes education through media and online channels, as well as sharing its latest research on employee actions that could compromise their employer's cyber security or data safety, and SME owners' attitudes toward cyber risk.

As well, IBC has created a self-assessment tool for SME owners considering a cyber insurance policy. This 10-question assessment can help business owners learn about the cyber security protocols and best practices that most cyber insurers look for when assessing risk. The assessment poses some of the questions that cyber insurers may ask during the application process.

The assessment and other resources for SME owners are available at **CyberSavvyCanada.ca**.

¹⁵ "The rise and fall of cyber policy growth," Canadian Underwriter, canadianunderwriter.ca/brokers/the-rise-and-fall-of-cyber-policy-growth-1004246818.





ibc.ca

