September 2023

The Canadian Cyber Insurance Market

IBC

Insurance Bureau of Canada

Introduction

Cyber insurance is a small but rapidly growing line of businesses for many Canadian property and casualty insurers. In 2022, cyber insurance became more accessible than it was in the previous year. According to 2022 data, 74% of organizations have cyber security insurance coverage, and 36% of those have a standalone cyber policy.[1] However, this number is likely lower for small businesses, and organizations with higher risk may still face difficulty in accessing coverage. As cyber threats continue to evolve, businesses – particularly small and medium-sized enterprises – will need more education on cyber security, resilience and how to qualify for cyber insurance.

State of the Canadian cyber insurance market

As cyber threats increase in frequency, magnitude and complexity, cyber insurance continues to evolve into a significant part of the commercial insurance market. However, with historically high claims cost pressure due to high frequency of cyber breaches and ransomware attacks, some insurers have reconsidered their scope of coverage, adjusted their underwriting standards or employed exclusions to better manage unknown and emerging cyber risks.

In 2015, insurers wrote $24.4 million in cyber premiums, and they are now writing more than $472 million in annual premiums.

While the size of the cyber insurance market has increased, the frequency and severity of claims have increased considerably faster. From 2020 to 2022, the combined industry loss ratio on cyber insurance averaged approximately 184% (see table below for combined loss ratios for each of the years from 2017 to 2022). This means that for every dollar insurers earned in premiums during that time, they paid out $1.84 in claims and operating expenses. After experiencing a hard market over the past few years, loss ratios improved in 2022, in part due to more rigorous underwriting. Given the uncertainty of the cyber landscape, it is difficult to predict if this positive trajectory will continue; however, it may be a sign that the cyber insurance market is maturing.

[1] CIRA, "Perceptions and Attitudes of Canadian Organizations Toward Cybersecurity," August 2022.

Cyber Insurance Financial-Year Results[2]

Year	Direct Premiums ($Millions)	Direct Claim Costs (Millions)	Combined Loss Ratio
2017	61	19	63.1%
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%**

What protection does cyber insurance provide?

Cyber insurance provides coverage against the frequent consequences of cyber events, including:

Data confidentiality breaches: Confidential or personally identifiable information is viewed, copied or stolen by an unauthorized individual or entity.

Ransomware and cyber extortion: Cyber criminals demand payment under threat of causing harm to the targeted entity (e.g., disabling their operations or compromising their confidential data).

Technology disruptions: A company experiences technology failure due to denial of service or other attack by a third party.

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

Legal and civil damages: the cost of legal representation and possible damages related to a privacy or network security breach

Security breach remediation and notification expenses: the costs to notify affected parties and mitigate potential harm from a privacy breach, such as providing free credit monitoring to affected parties

Forensic investigations expenses: the costs of hiring a firm to investigate the root cause and scope of a data breach

Computer program and electronic data restoration expenses: expenses to restore or recover damaged or corrupted data caused by a breach, denial-of-service attack or ransomware.

[2] Source: IBC with data from MSA, all companies.

[3] In 2022, some 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.

Cyber coverage

Cyber insurance products are provided in one of three ways:

1. **Stand-alone cyber insurance policies** (policies specifically for cyber risks) are the most common cyber policies in Canada, the United States and Europe.
2. **Coverage for cyber events may be included in a traditional property and liability insurance policy.** These policies typically have very low limits that would not cover the full cost of a breach or cyber attack.
3. **Endorsements (also known as riders)** can add, remove or exclude certain cyber coverages, altering a cyber or traditional insurance policy to meet specific needs.

Silent cyber risks

Silent cyber, or "non-affirmative" cyber, risks are neither expressly covered nor excluded in an insurance policy.

Unlike stand-alone cyber insurance, which clearly defines the parameters of cyber coverage, many traditional policies do not specifically refer to cyber risks. This means that a policyholder looking for cyber coverage should not rely on traditional commercial policies to cover cyber risks. Many insurers have introduced specific exclusions for cyber, as these traditional products were never intended to cover cyber risk. Ideally, affirmative stand-alone cyber coverage will clearly define what is and is not covered. Otherwise, policyholders could be responsible for paying out of pocket for cyber losses in certain circumstances.

Silent cyber risk is a critical issue for insurers and their customers alike. It can represent a significant, unexpected risk to insurers' portfolios, exposing them to catastrophic losses stemming from risks they neither underwrote nor charged for. Commercial clients may not understand what is covered and excluded in their policy, resulting in coverage uncertainty. Some businesses may believe that they have adequate coverage for cyber risk when they do not.

To help address this confusion, many insurers have clarified their coverage intent by defining cyber risk and excluding it from non-cyber policies. In early 2022, IBC finalized a new IBC Cyber Loss Exclusion Endorsement. This endorsement clarifies exactly what is excluded under cyber losses, helping policyholders better determine if they need broader coverage.

IBC also uses media and online channels to help business owners, particularly those who rely on their online presence and e-commerce, better understand cyber coverage. IBC encourages business owners to work with their insurance representatives to find coverage that will provide them with optimal protection and perhaps even provide them with safe cyber security procedures.

IBC's role in promoting cyber resilience

Incidents of cyber crime – particularly ransomware attacks – have drastically increased since remote work became commonplace due to the COVID-19 pandemic. As more people began to work from home, criminals began to prey on them. And as many small businesses adopted digital processes and moved some of their business online, cyber criminals found yet more opportunities.

IBC offers [free resources to businesses] and suggests best practices to improve their cyber health. Business owners can also protect themselves by:

- **Enforcing multi-factor authentication for log-in and network access** (i.e., requiring a password and at least one more step to log in, such as sending a code to a mobile phone)
- **Focusing on email security**, such as enabling attachment scanning, using external sender banners and training staff to identify and contain malicious phishing attempts
- **Running regular data backups and encrypting data** that is stored or in transit.

IBC also recommends business owners visit the [Canadian Centre for Cyber Security website], which provides information to businesses on reducing exposure to cyber threats.

IBC produces annual awareness campaigns to help educate consumers on cyber risk. The 2022 campaign focused on educating business owners and their employees on improving cyber hygiene. This campaign included a Cyber Savvy Report Card based on an Angus Reid survey that graded employees of small and medium-sized businesses on their actions and knowledge about cyber risk and security.

In 2023, IBC will update its Cyber Savvy Report Card research and continue to engage business owners to help them better understand their cyber risk and learn more about accessing cyber insurance.

ibc.ca