Cyber Risk and Insurance: Managing Cyber Risks in Today's Evolving Threat Landscape

The Insurance Brokers Association of Canada (IBAC)

August 2023

Table of Contents

Key Terms & Definitions

Software and General Cyber Key Terms (1/3)

Misconfiguration: An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.

Software Vulnerability: A design flaw or implementation error within an application or system that presents an exploitable weakness.

PII (Personally Identifiable Information): PII refers to sensitive data that can identify individuals, such as names, addresses, social security numbers, and email addresses. Protecting PII is essential to prevent identity theft and privacy breaches. Security measures, like encryption and access controls, are crucial to safeguarding this information

Remote Desktop Protocols (RDP): A network communications protocol enabling network administrators remote access to users' physical desktops.

Security Patch: A "repair" for a piece of programming, which can also be known as a "fix." A patch is the immediate solution provided to users, and can sometimes be downloaded from the software maker's website.

Zero-day Vulnerability: A vulnerability previously unknown to the vendor, commonly associated to a vulnerability first discovered by a threat actor.

Trusted Third Party: An entity awarded privileges to perform certain services, manage IT assets, able to expand an organization's attack surface beyond it's immediate control.

EDR: An endpoint security solution that continuously monitors devices to detect and respond to cyber threats like ransomware and malware.

Software and General Cyber Key Terms (2/3)

Virtual Private Network (VPN): A VPN creates a secure connection for users to access private networks over the internet, safeguarding data and privacy. It encrypts communication and shields online activities from potential threats and surveillance.

Human Access: Human access involves individuals interacting with digital systems. Secure management of human access includes authentication measures like passwords and biometrics, ensuring proper authorization and preventing unauthorized use.

Non-Human Access: Non-human access involves automated systems and devices interacting with digital environments. Strong authentication and access controls for non-human entities prevent misuse and exploitation of vulnerabilities, bolstering system security.

Least Privilege: Least privilege enforces minimal access rights necessary for users and entities to perform tasks. By limiting unnecessary access, the impact of breaches is reduced, enhancing overall security by minimizing potential damage.

NIST (National Institute of Standards and Technology): NIST provides standards and guidelines for cybersecurity, helping organizations manage risks, detect threats, and respond effectively. NIST's framework covers areas such as risk management, incident response, and security awareness, improving overall information and asset protection.

Social Engineering: The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.

Key Terms & Definitions

Software and General Cyber Key Terms (3/3)

SIEM: A solution that aggregates event data across IT systems within a network. It identifies anomalies and raises alerts of potential/actual incidents & is monitored by a SOC with the authority to respond accordingly.

Minimum Controls: Minimum controls are fundamental security measures that organizations must implement as a baseline defense. These controls, including firewall configuration, patching, and access control, establish a foundation for cybersecurity, mitigating common threats and vulnerabilities.

Key Legislations in Canada

Bill C-27: The Digital Charter Implementation Act, containing legislation relating to consumer privacy, data protection, and artificial intelligence (AI).

Quebec Bill 25: An act to modernize legislative provisions as regards the protection of personal information.

Cyber Insurance Coverage Terms

See slides 35 to 39

Cyber Threats Key Terms

Ransomware: A form of malware that renders information and IT systems inaccessible through encryption, threatening to steal and publish sensitive information. This enables threat actors to demand large sums of money through cryptocurrency in exchange for re-gaining access to systems and avoiding a data breach.

Malware: A piece of computer code designed to interfere with IT systems in a malicious way.

Business email compromise: a type of email scam that occurs when a threat actor spoofs or gains access to an business email account. The threat actor, posing as a trusted entity, emails their target requesting that they transfer funds to a 'new' account, or take similar action.

There are many ways this attack can occur, with criminals posing as employees, customers, vendors, or any entity that might be expected to request funds to an account as part of regular business processes.

Insider Threats: Disgruntled users and employees that use their credentials, privileges, and knowledge of internal networks to sell their information to the cyber criminals.

Hardening: A process intended to reduce attack surface by securing IT systems through recommended configurations according to vendor product requirements. CIS benchmarks are industry standards for hardening vendor products [27].

Click on each underlined element to be directed to first slide mentioning this term

Section 1

Current and Emerging Cyber Risks

Overview: Current and Emerging Cyber Risks

A complex cyber threat landscape, driven by a chain of motivated threat actors, keeps organizations up at night. In this section, we look to uncover **the impact of the cyber threat landscape on Canadian organizations**, focusing on Small & Medium sized Enterprises (SMEs) [1].

Key Topics and Questions Addressed

1) **The cyber criminal supply chain**
   - Who are the threat actors responsible for cyber attacks globally, and within Canada?
   - What motivates threat actors to target and exploit organizations?

2) **All industries are at risk**
   - What industries are targeted by threat actors?
   - Case studies from recent high-profile incidents in Canada

3) **SMEs are not 'too small' to be targeted**
   - What challenges do SMEs face when managing cyber risk?
   - What opportunities do SMEs present for cyber criminals?

4) **Impact of a cybersecurity incident**
   - What are the real costs of a cyber incident?
   - How could an incident disrupt an organization's operations and trusted relationships?

5) **Understanding the kill chain of a ransomware attack**
   - What methodology do threat actors use conduct a ransomware attack?
   - What are the key phases to a ransomware attack?

6) **The issue of residual risk**
   - How do threat actors gain an initial foothold in an organization?
   - Why is there a need for cyber insurance?

$5M+

The average cost of a cyber attack in Canada. [2]

19%

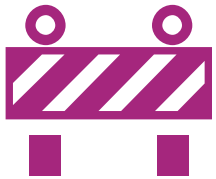
of businesses saw a **material impact on their reputation** following a cyber attack. [3]

14%

of SMEs feel prepared to face a cyber attack. [4]

32%

of recorded cyber attacks have led to a **halting of day to day operations**. [3]

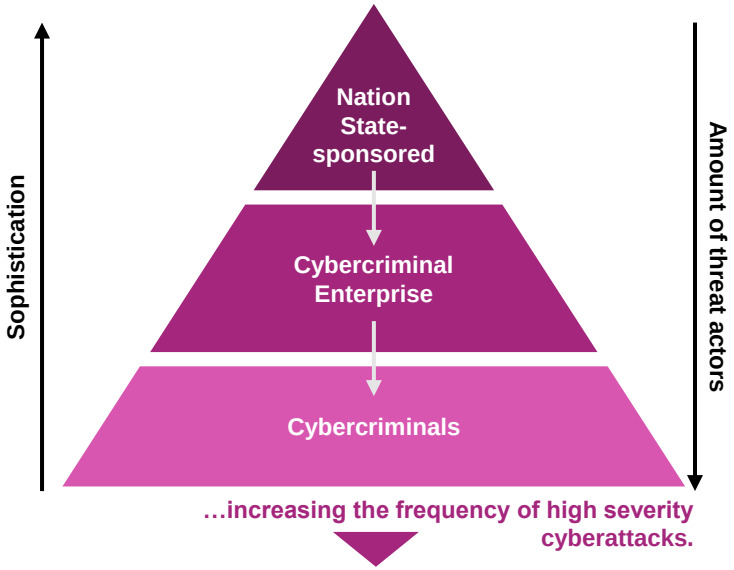


Click on each underlined element to be directed to a slide providing further details

The Cyber Criminal Supply Chain

A cohesive network of cybercriminals poses significant risk to SMEs**. Different threat actors co-exist within the current threat landscape, as top-level actors grab headlines and grant low exposure to their smaller counterparts.**

Highly sophisticated cyber attack techniques are being passed down to lower-level threat actors…



…increasing the frequency of high severity cyberattacks.

Nation State Sponsored: groups are suspected of operating with the support of nation states, free from domestic law enforcement. Note that the key term here is suspected – it is difficult to legally determine whether a ransomware group is tied to a nation state.

Cybercriminal Enterprise: organized crime groups which operate their attacks using malware created by their own developers. They are big players in the Ransomware-as-a-Service ecosystem (RaaS), and can leverage a wide network of affiliates to use their newly developed RaaS in return for a fee.

Cybercriminals: individuals/small groups whose attacks and activities are facilitated by the cyber criminal supply chain (*RaaS kits come with operating support*). Pricing can range from $40/month to several thousands, a low fee relative to potential gains from a successful ransomware attack. [6]

Sophisticated threat actors at the top of the supply chain develop malware for their own exploits, before making these same technologies available to lower-level threat actors through the dark web.

This trickle-down effect means that anyone can access the tools necessary for committing cyber crime. It can be expected that cyber crime levels will increase in times of economic hardship, as new players enter the frontlines.

Cyber criminals share a common motivation: financial gain**.**

Previously achieved through large scale data breaches and the rewards of selling data on the dark web, the vast supply of data available has driven black-market value down.

The recent shift to ransomware extortion demonstrates the financial opportunism of threat actors, and ensures that all organizations with a balance sheet are attractive targets.

Takeaway

- An increasingly **interconnected threat actor landscape**, the affordability of **RaaS kits**, and the **potential return on investment** a cyber threat campaign can generate are motivating threat actors.
- In 2020 and 2021 alone, ransomware groups made over $765M in profit, globally. [5]
- Headlines focus on big names, but **the reality for SMEs is often not widely reported on.**

All Industries Are at Risk

Industries Most Targeted by Cyberattacks in 2022, with recent Canadian examples [7]

09/2019: A Crown Corporation, responsible for the Defence department's projects and infrastructure, was hit with a cyber attack. [8]

Impact: Disrupted computer systems, resulting in ongoing issues with procurement and other projects.

02/2023: A retailer suffered an incident which left its website and electronic payment systems offline for multiple days. [10]

Impact: In-store orders could only be paid in cash. Unable to accept electronic payments, gift cards or handle returns.

06/2023: An energy company suffered a cyber attack resulting in gas stations being unable to accept credit or debit payments for multiple days. [12]

Impact: Suspended electronic payment & loyalty points, expected to cost millions in damages.

Services
20%

Public Sector
10%

Information & Technology
8%

Retail
8%

Energy & Utilities
6%

Manufacturing
16%

Construction
8%

Healthcare
8%

Finance
6%

Transportation
4%

01/2023: An automotive components manufacturer, experienced cyberattacks that spread across its network. [9]

Impact: Production was disrupted across three of its factories, and took over 2 weeks to be restored sustainably.

12/2022: A children's hospital was hit by a ransomware attack and forced to shut down most of its systems, including phone lines and staff payroll. [11]

Impact: Severe delays in laboratory, imaging services, and surgeries, directly affecting patient care and health.

** 'Other' industries account for the remaining 6% of cyber attacks across Canada*

Takeaway

- Data shows that **all industries are being targeted by threat actors.**
- Due to their common financial motivations and the return on investment threat actors can achieve, **organizations with weak cybersecurity controls are being targeted**, rather than specific industries.

SMEs are not 'Too Small' to be Targeted

While organizations with large amounts of data have been traditionally targeted by threat actors, ransomware has since changed their focus**. Now, financial rewards and ROI models drive criminal behaviour.** Organizations with weak security are easy targets to threat actors.

43% of global cyber attacks aimed at SMEs

Coveware releases quarterly ransomware reporting on a consistently measured metric: **Impacted Companies by Employee Count.**

In 2023, organizations with **1-100 employees account for 30.3%** of incidents, while organizations with **101-1000 employees account for 35.7%** of incidents. [13]

Reports from early 2023 show incidents from 1-100 employee organizations decreasing to 27%, while the attack frequency for organizations with 101-1000 employees has increased. [13]

The high percentage of cyber incidents confirms that **SMEs appear more likely to fall victim to cyber attacks**. [14]

SMEs are considered to be highly lucrative for threat actors, since they create opportunity for low-risk, high frequency attacks.

SMEs can view cybersecurity as an unnecessary additional cost that can fall behind business growth priorities.

This mentality results in weak cybersecurity maturity and financial capacity. This allows for weaknesses and vulnerabilities which cyber criminals exploit.

Only 14% of SMEs are correctly prepared to defend themselves against cyber threats. [14]

Other threat actors will pay close attention to small organizations that allow them to access bigger targets, and reap the high rewards a single attack can generate.

Some SMEs find themselves targeted by threat actors due to their position within the supply chain.

Managed service providers are considered initial gateways to a larger pool of target organizations (particularly technology service providers). They become attractive options for sophisticated threat actors looking to maximize their ROI for a single attack.

The **Kaseya incident** in 2021 offers a high-profile case study for this threat. **Malware was hidden in a software update and proliferated across the Kaseya client base.** [15]

Reducing the volume of common vulnerabilities and weaknesses in an organization's cyber defence is only possible when:

Organizations invest in : **people, processes, and technologies.**

To : **prevent**, **detect, and respond** to a cyber attack.

Takeaway

- SMEs exhibit a **higher likelihood for common vulnerabilities** relative to larger organizations (frequency of cyberattacks).
- This makes SMEs 'low hanging fruit' for financially motivated threat actors, evidenced by statistics proving **that headlines do not reflect the reality of cyber threats for SMEs.**

Impact of a Cybersecurity Incident

It is important for organizations of all types to understand the impact of a major cyber incident. **Reported in averages, the real experience of individual organizations varies significantly according to their ability to prevent, detect, respond to cyber incidents.**

Direct

$5M+

The average cost of a cyber attack in Canada.

=

Ransomware incidents can leave businesses…

- Unable to access critical IT systems or services.
- Losing productivity (whilst still paying overheads).
- Losing income loss due to business interruptions.

The average estimated time taken to contain ransomware was 89 days in 2022. [16]

+

Other direct costs to managing cyber security incidents include:

- Costs of the response effort.
- Legal advice.
- Notifications to customers and regulators.

Indirect

The regulatory landscape has continued to evolve, increasing pressure to comply with information security requirements.

Upcoming privacy regulations:

- **Federal Bill C-27** (currently being read in parliament), will likely introduce the *Consumer Privacy Protection Act* specifying fines (the greater sum of either 5% of revenues or $25M), and being enforced by a *Personal Information and Data Protection Tribunal*. [17]
- **Quebec's Bill 25**, requiring information protection and handling, enforced by significant penalties in case of non-compliance.
- **B10 guidelines** for Financial Service organizations from the Office of the Superintendent of Financial Institutions (OSFI). Focused on third party risks and the importance of managing them. [18] Third party risk due diligence is forecasted to be built into future OFSI regulations.

Reputational damage can entail many consequences for a business, although quantifying it remains challenging.

- **Company Value**: Public cyber incidents have a short-term impact on company valuations, although recoverable. [19] Public perception of ransomware attacks has matured in recent years, facilitating this process. [20]
- **Delays in Negotiation**: Ransomware attacks mainly concern businesses in the process of acquisitions or partner negotiations. Business email compromise and fraudulent instructions shared between partners lead to tense conversations, and challenges relationship management.
- **Trust**: Business partners place each other in position of trust, often sharing sensitive information and network access with the expectation that this will be protected. A cyber incident can break that trust, causing financial loss to a partner organization – all organizations seek to avoid this risk.

Takeaway

- Cyber incidents entail **material financial costs** for a business, whether through **operational disruption**, **regulatory compliance**, or **reputational damage**.
- These costs can reach **hundreds of thousands of dollars for SMEs**, with the average cost of an incident in Canada being **CA$5M**.
- Cyber insurance is therefore necessary for all organizations to protect the balance sheet.

Understanding the Kill Chain of a Ransomware Attack

Ransomware results from prolonged effort by threat actors who **follow a common methodology** to establish a position where ransomware will be effective. It is important that organizations **understand this methodology to inform their risk management decisions**.

01. Reconnaissance

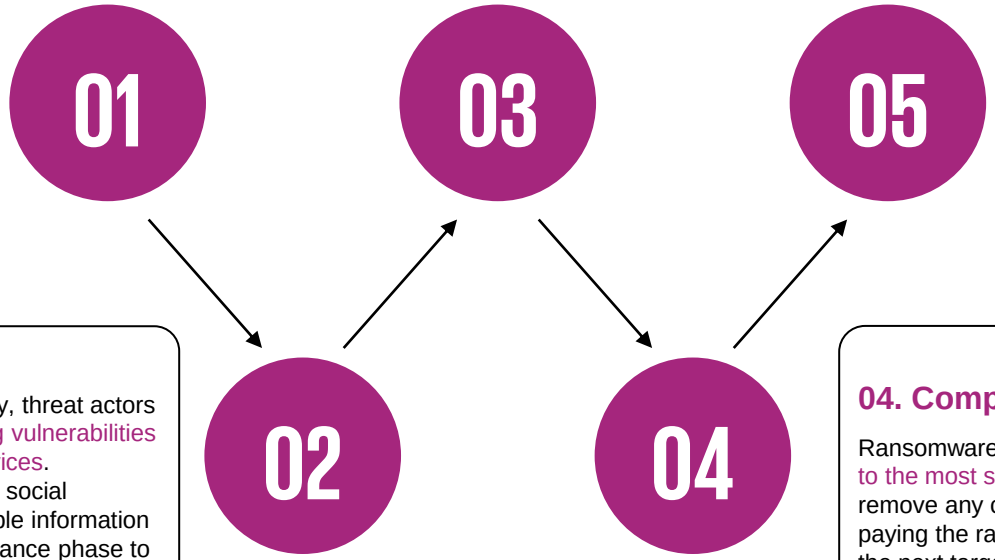
Threat actors use technology platforms and online sources to research publicly available information, offering an insight to the organization's attack surface. Threat actors are easily able to identify exposed applications and services belonging to the company, as well as information on employees to assist social engineering efforts through platforms, such as LinkedIn.

02. Gaining Access

With a view of the target company, threat actors seek to gain access by identifying vulnerabilities and weaknesses in exposed services. Employees will be tested through social engineering using publicly available information discovered during the reconnaissance phase to evade detection, while misconfigurations in exposed services or applications will be targeted.

03. Establishing Persistence

Once inside, threat actors seek to expand their access levels, moving laterally and deploying remote access tools (RATs) to cement a persistent foothold in the target network.



04. Compromise and Escalation

Ransomware requires administrative access to the most sensitive parts of the network to remove any chance of the organization not paying the ransom. Escalation of privileges is the next target for threat actors, to gain the keys to the kingdom.

05. Achieve Objectives

Having gained sufficient administrative privileges and access to critical systems, databases, and backup servers, the threat actor is ready to detonate the ransomware.

Takeaway

- Ransomware results from **planned, well-structured,** and **prolonged efforts** by threat actors.
- Threat actors commonly use **similar kill chain methodologies**, leveraging different phases to execute an attack. Organizations must understand what these different phases entail to **inform their risk management decisions**.

Why Cyber Insurance? - The Issue of Residual Risk

When conducting reconnaissance and seeking to gain access to an organization, threat actors rely on cyber weaknesses and vulnerabilities. **Some risks can be managed by an organization, whilst others are out of their control, presenting residual risk.**

By understanding common weaknesses and vulnerabilities that lead to cybersecurity attacks, organizations can focus their efforts on risk mitigation, investing in resources to achieve security objectives and enable operations.

Human Error significantly challenges cybersecurity risk management (*e.g.: stolen credentials for network access, phishing/social engineering attacks, insider threat misuse, misc. IT management errors*).

Vulnerability Management : vulnerabilities are identified and disclosed to vendors who then develop, test, and release a patch remediating the vulnerability. Exploitation of software vulnerabilities continues to be a leading cause of cybersecurity incidents (*45% of incidents*). [23]

IT System Misconfigurations enable access to internet-facing IT systems and applications (*25% of cyber incidents are caused by miscellaneous errors, of which 15% are misconfiguration errors*. [21] *Poorly secured Remote Desktop Protocols (RDP) account for 29% of incidents).* [22]

Social Engineering has consistently been a primary source of incidents in recent years. While only 2.9% of users click on phishing emails, it is sufficient to compromise a network and provide threat actors with the initial access needed to initiate their kill chain. [21]

However, organizations have little control when dealing with…

Zero-Day Vulnerabilities

All organizations face the risk of unknown flaws in software or hardware that lack official fixes (called zero-day vulnerabilities) being exploited by threat actors.

The lack of awareness surrounding zero-day vulnerabilities, gives attackers the advantage of exploiting them before anyone can respond. Developing a patch for a zero-day vulnerability takes time, and leaves systems exposed during the investigation, and deployment phases.

Third Party Risk

Managed service providers offer great value to SMEs, providing access to expertise without related overheads. The close nature of these relationships often means sharing network access privileges and sensitive data.

In addition, the extent of control an organization has on its trusted third parties is limited. If a trusted third party suffers a cyber incident, their clients can quickly find themselves impacted.

Takeaway

- **People, processes, and technologies** must work together to **prevent, detect, and respond** to cyber incidents.
- Managing cyber risk is complex, and residual risks (*zero-day vulnerabilities, third party risks, and misconfigurations/human error*) will impact businesses despite good controls. This cements the need for cyber risk transfer through insurance.
- Log4j and MOVEit are two high-profile cases illustrate the fact that residual risk cannot be completely eliminated. [24] [25]

Takeaways: Current and Emerging Cyber Risks

SMEs face challenges in **dedicating the necessary resources to manage cyber risks**. Although risk mitigation is within an organization's control, residual risk remains inevitable. **Risk transfer through cyber insurance is therefore necessary to maintain a comprehensive cyber risk management strategy**.

Summary of Key Topics and Questions Addressed

1) **The Cyber Criminal Supply Chain: a trickle-down effect**
   - Cyber threat actors vary in their sophistication and funding. Top-level actors enable their smaller counterparts through the distribution of malware on the Dark Web.
2) **All Industries are at Risk: threat actors do not discriminate**
   - Incidents impact all industries. Financially motivated, threat actors target organizations prone to vulnerabilities, achieving a lucrative ROI with ransomware.
3) **SMEs are not 'Too Small' to be Targeted**
   - SMEs often present low hanging fruit for threat actors, as tight budgets, lack of expertise, and resources lead to easily exploitable vulnerabilities and weaknesses.
4) **Impact of a Cyber Incident**
   - Organizations suffer material losses and financial consequences as a result from cyber incidents. Insurance is crucial to protecting businesses during a crisis.
5) **Understanding the Kill Chain of a Ransomware Attack**
   - Threat actors follow a common methodologies to gain a foothold within an organization and launch a series of attacks, often leading to ransomware.
6) **The Issue of Residual Risk**
   - Threat actors utilize common weaknesses and vulnerabilities. Organizations can gain awareness to protect themselves against these elements, mitigating risk.
   - Cyber insurance is crucial, as certain elements are outside of an organization's control and result in residual risk.

Additional Examples of Canadian Companies Targeted by Cyberattacks in 2023

Yellow Pages

April 2023

- Scans of **employee passports and driver licenses.**
- Employee's **Social Insurance Numbers.**
- Budget and debt forecast.

GATEWAY CASINOS & ENTERTAINMENT LIMITED

April 2023

- A ransomware led to **5 days of interruptions** in the operations of **50% of their locations.**
- Uncertainty of leaked client and employee information.

Indigo Books · Gifts · Kids

May 2023

- **Lost over a month of online sales** because of a ransomware.
- The company estimated the **cost of the attack to be over $5M.**

Click on each underlined element to be directed to a slide providing further details

Section 1 - References

P. 6	[1] *Innovation, Science and Economic Development Canada (ISED)* defines an SME as a business establishment with 1 to 499 paid employees. [2] IBM, *Cost of a Data Breach Report*, 2022 [3] CIRA, *CIRA Cybersecurity Survey*, 2022 [4] Accenture, *The Cost of Cyber Crime*, 2023
P. 7	[5] Bleeping Computer, *Ransomware Profits Drop 40% in 2022 as Victims Refuse to Pay*, 2022 [6] Crowdstrike, *Ransomware-as-a-service (RaaS) Explained*, 2023
P. 8	[7] PwC Canada, *Canadian Cyber Threat Intelligence Annual Report*, 2022 [8] Ottawa Citizen*, Defence Construction Canada Hit by Cyber Attack*, 2019 [9] The Star, *Exco Technologies Hit by Cybersecurity Incident at Three Factories*, 2023 [10] Insurance Business Mag, *Running Room Canada Targeted by Unauthorized Group Customer Data*, 2023 [11] Global News Ca., *Ransomware Attack SickKids Toronto*, 2022 [12] The Star, *Some Petro Canada Locations Only Accepting Cash After Cybersecurity Incident*, 2023
P. 9	[13] Coveware, *Analysis across Ransomware Quarterly Reports since 2021,* 2023 [14] Accenture, *Cost of Cyber Crime*, 2023 [15] The Record, *REvil ransomware gang executes supply chain attack via malicious Kaseya update,* 2021
P. 10	[16] IBM, *Cost of a Data Breach Report*, 2022. [17] DLA Piper, *Data Protection Laws Around the World*, 2023 [18] OSFI, *Third Party Risk Management Guideline*, April 2023. [19] Harvard Business Review, *The Devastating Business Impacts of a Cyber Breach*, 2023 [20] Bleeping Computer, *Ransomware Profits Drop 40% in 2023 as Victims Refuse to Pay*, 2023
P. 12	[21] Verizon, *Data Breach Investigations Report*, 2022 [22] Blakes, *Canadian Cybersecurity Trends Study*, 2022 [23] Blakes, *Canadian Cybersecurity Trends Study*, 2023 [24] Bleeping Computer, *New Zero-Day Exploit for Log4j Java Library is an Enterprise Nightmare*, 2021 [25] Bleeping Computer, *New MOVEit Transfer Zero-Day Mass-Exploited in Data Theft Attacks*, 2023

Section 2

The Cyber Insurance Landscape

Overview: The Cyber Insurance Landscape

Cyber insurance is a necessity, due to the complexities of the cyber threat landscape and the **pressing issue of residual risk.** In this section, we discover the way in which cyber insurance has grown to become **a valued tool for risk management.**

Key Topics and Questions Addressed

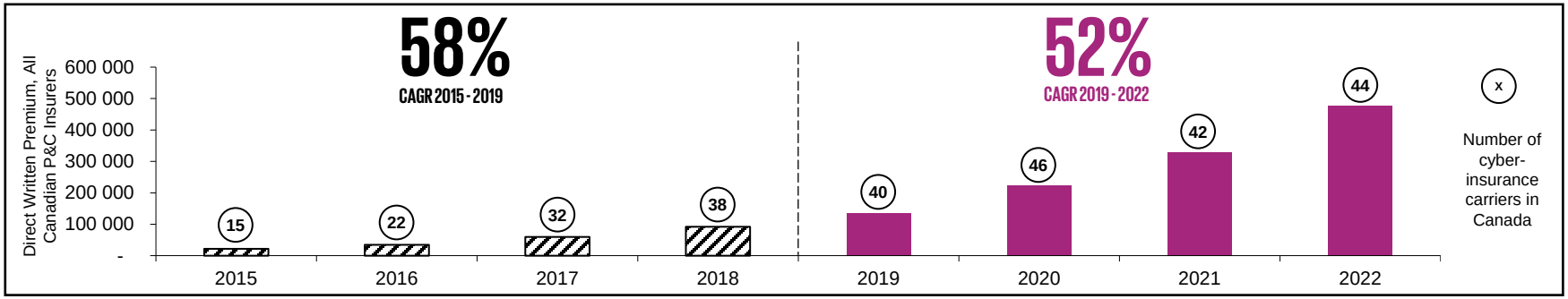
1) **A history of cyber insurance**
   - What elements characterized the early Canadian cyber insurance market?
   - What did earlier cyber insurance policies cover, and who were the main buyers?
   - How has the cyber insurance market developed over time to where we are today?
   - What were the key trends and challenges during the 2010s and early 2020s?
2) **The question of viability**
   - How has the evolving cyber threat landscape impacted the cyber insurance market?
   - How have cyber insurers adapted in the wake of ransomware-as-a-service?
3) **Cyber insurance today**
   - What opportunities does the new cyber market present for insurance providers?

Loss ratios [1]

Year	Loss Ratio
2015	33%
2016	11%
2017	31%
2018	45%
2019	87%
2020	268%
2021	98%
2022	-28%*

Impact of RAAS

The spike in losses around 2020 caused cyber insurance **viability** to be questioned. Market corrections serve to enhance the **sustainability** of cyber insurance. [1]



Despite a slight slowdown, cyber insurance remains one of the **fastest growing lines of business within the insurance industry**. The **rapid increase in premiums mirrors the rise in demand**, due to the increasing frequency and severity of cyber attacks. [1] Although the **number of insurers offering cyber insurance in Canada increased threefold** (*from 15 in 2015 to 44 in 2022*) **the market remains concentrated**. In 2022, the top 10 insurers (*by direct premium*) made up 95% of direct premiums in 2022.

* Negative direct claims in 2022 per MSA data are driven by large negative losses reported by Lloyd's. This is likely due to the release of reserves due to favorable claim activity

Click on each underlined element to be directed to a slide providing further details

1990s & 2000s – Rapid Start for Cyber Insurance in Canada

The market for cyber insurance was born in the 1990s, with its growth accelerated by increases in data breaches. **Originally an add-on, cyber insurance transitioned to a standalone product** by improving data management and quality practices through the 2000s.

1997 - Launch of Internet Security Liability Insurance

The predecessor to cyber insurance, Internet Security Liability (ISL) was launched by Steve Haase, a US-based AIG agent. Resulting policies were originally aimed at online retailers, such as Amazon, that were collecting and storing their customers' credit card numbers. [2]

Early Cyber Policy Coverage

The early cyber insurance products' coverage focused **on 3rd party liabilities resulting from data breaches**. For that reason, it was not very popular with businesses who felt that they did not carry sufficiently large amounts of Personally Identifiable Information (PII) [4] to justify the purchase.

2000 to 2005 - The Arrival of Cyber Insurance in Canada

Companies in Canada started to become more aware of the potential threat and impact of cyber attacks, due to the increasing frequency and gravity of data breaches.

As such, insurance companies started to offer cyber insurance add-ons to existing commercial insurance policies. [2]

State of the Canadian Market

In the early 2000s, **only a few major insurers offered cyber insurance policies** (e.g. AIG, Chubb). The market remained undeveloped, with demand mostly generated from larger businesses responsible for storing or processing large amounts of customer data. [3]

Takeaway

- Most Canadian insurers observed sizable losses on individual policies, with **severe and high-profile data breaches costing them tens of millions of dollars**.
- **The frequency of these losses was manageable however,** and cyber insurance was still considered **an exciting new class** attracting capacity to the market.

2010 to 2019 – The Perfect Storm

High severity data breaches resulted in new regulations, as governments sought to improve protections of customer information. Cyber insurers **began to provide services that would assist organizations** in responding to data breaches and regulatory requirements.

High-Profile Incidents Shape the Regulation of Customer Information Protection in Canada

2011 – Sony: 77M records stolen from the PlayStation Network. [5]

2015 – Ashley Madison: 60GB of data stolen from the sites 32m users, resulting in extortion threats sent to users. [6]

2016 – GDPR: EU data protection regulations introduced strict requirements for protecting & handling customer data, and significant fines for non-compliance.

2017 – PIPEDA: Canadian federal regulation was introduced, including mandatory data breach notification and reporting requirements for Canadian businesses.

In reaction to headlines, cyber insurance buyers flooded the market. Industries with high data breach risk remained the biggest buyers.

The Cyber Insurance Market's Reaction

Increase in demand for cyber insurance products due to:

- The evolution of the threat landscape.
- The regulatory and legislative environment.
- Increase in added value within new product and service offerings.

New buyers enticed by **new coverage offerings**:

- Business Interruption.
- Cyber Crime.
- Cyber extortion.

Most valuable for industries unconcerned with customer data breaches (Energy, Logistics, Manufacturing). [7]

Low awareness & understanding of risk profiles within cyber insurance books.

Application forms used to underwrite cyber risk lacked technicality. This enabled portfolios to grow significantly, although mis-assessing risk severity and frequency.

Insurers began to recognize that clients needed support, not only cash. **Post-incident services were introduced** to support organizations.

A key unique selling point (USP) for the product, insurers began to offer panels of experts to help businesses manage cyber incidents.

Takeaway

- **Losses rose steadily over this period**, with Business Email Compromise and Ransomware beginning to have an impact.
- The general sentiment, however, maintained that **the frequency and severity of losses was manageable**.
- Cyber premiums were seen as a way to offset losses across Property, Auto and D&O lines, triggering **a highly competitive 'soft market.'**
- **A 'race to the bottom' unfolded, resulting in broader coverage**, cheaper premiums, and limited underwriting scrutiny.

2019 to 2021 – Will Cyber Insurance Ever be Viable?

2019 initiated a period of turbulence for cyber insurance, with a loss environment driving market correction. As organizations found it increasingly challenging to get cyber insurance, and cyber insurers pulled capacity, many began to **question the product's viability.**

Global Events Impacted the Industry in Different Ways

2019 - Ransomware-as-a-Service (RaaS)

Sophisticated threat actors began to license their ransomware programs on the dark web to lower-level criminals, leading to the rise of RaaS. Financially motivated actors targeted all organizations with a balance sheet, shifting the threat landscape in a way that the cyber market was not ready for. [8]

2020 - COVID-19

The Covid-19 pandemic forced businesses to quickly adapt to work-from-home requirements. The rush to implement remote work technologies meant expanding an organization's threat surface, with the risk of misconfiguring solutions due to emergency conditions. RDP and Virtual Private Network (VPN) vulnerabilities were in abundance.

113%

Canadian loss ratio in the second half of 2021. [9]

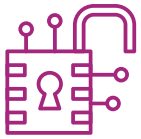
700%

Growth in the average ransom payment from 2019 – 2022. [10]

The frequency and severity of losses crippled underwriting performance.

- Business email compromise and ransomware attacks were energized by pandemic conditions.
- Insurers raised their awareness of the nature of the risk they had onboarded at very low prices in previous years.
- Some insurers pulled capacity, while others embarked on a market correction to reduce losses.

The market had a significant correction towards technical underwriting.



- New minimum control requirements introduced by insurers forced organizations to invest in cybersecurity to offset punitive terms and conditions.
- Coverage restrictions such as co-insurance on ransomware were introduced to manage risks which were not meeting these new minimum standards.

A sharp reduction in primary layer capacity and risk appetite.

- Cyber insurance had entered a 'hard' market.
- Premiums and retentions rose sharply, creating pressure on organizations looking to move their workforce remote and dealing other with business costs created by the pandemic.

Takeaway

- The market correction was necessary to **sustain the cyber insurance market.**
- Brokers **should not expect premiums or risk assessments to return to pre-RaaS levels** (pre 2019).
- Brokers need to be able to **guide their clients through the technical requirements of underwriters** to ensure a stable market.

Cyber Insurance Today – A Stabilized Market

The question of viability has dominated headlines, but **ignores the realities of cyber underwriting pre-2021**. Since then, the market has corrected itself, **and has established a more mature and sustainable approach for clients both now and in the future.**

Key Trends in the Current Market [11]

Demand for Standalone Insurance remains high for cyber insurance products, driven by the evolving threat landscape and regulatory environment.

New Coverage Restrictions were introduced by insurers to manage undesirable risks. Co-insurance on ransomware, system neglect conditions, and systemic risk exclusions were also brought forward.

External Vulnerability Scans are being leveraged by underwriters to identify weaknesses that can be exploited by threat actors, both during the underwriting process and the policy period.

Pre-Incident Service Offerings are being pushed by brokers and insurers to help clients mitigate their cyber risk to improve their insurability.

Technical Questions and Underwriting Appetite have replaced short application forms by targeting key controls for risk prevention**,** giving underwriters the tools required to better select risks to manage their portfolios**.**

More and more underwriters are adopting technical measures

Underwriters inform their risk selection by:

- Demanding minimum controls.
- Leveraging new technologies for evaluation.

This has created challenges for SMEs who are struggling to obtain favorable insurance terms and conditions, opening up a brand new field of pre-incident services that help SMEs mitigate cyber risk and meet these expectations.

Insurtechs are growing rapidly in Canada [12]

Insurtechs companies approach the cyber insurance industry from both sides of the risk mitigation/transfer equation. Cyber-focused insurtechs tend to be cyber security experts first, and insurers second.

By combining vulnerability scans, risk assessments, and controls with insurance products, insurtechs can write risks other insurers may not, on the basis that risk mitigation services are also taken up.

Traditional insurers are reacting by increasing their services

Traditional cyber insurers are beginning to offer services through 3rd parties, helping clients improve their risk posture:

- Vulnerability scans.
- Dark Web monitoring.
- Discounts on key security solutions.

Brokers are encouraged to push clients to use these services when required, while demanding that insurance companies reward them with favorable terms and conditions.

Takeaway

- Brokers must be capable of supporting their clients in the new market. Brokers **need an understanding of the risk management requirements of underwriters**, and to ensure that they have solutions on hand to help organizations meet these requirements.
- **Risk transfer is not possible without effective risk mitigation**, and residual risk means one cannot work without the other.
- In Section 3, **the role of the broker in this new market will be unpacked**.

Takeaways: Cyber Insurance Landscape

The last decade has seen the **cyber insurance market evolve, mature, and adjust to client needs and the changing threat landscape**. It is important that the market stay this course, and **find new ways to blend the lines between risk mitigation and transfer.**

Summary of Key Topics and Questions Addressed

1) **A History of Cyber Insurance**

- Throughout its short history, the market has adapted to provide coverage and services to meet clients' needs, from initially servicing organizations concerned with data privacy regulations to supporting those concerned with business continuity and income loss.
- Despite high-profile data breaches in the 2010s, the severity and frequency of losses made cyber insurance an attractive line of business for insurance companies battling Auto, Property and D&O claims. Softer underwriting practices and competition drove the conditions that would leave the market underprepared for the changing threat landscape.

2) **The Question of Viability**

- The rise of Ransomware-as-a-Service, combined with the pandemic, shifted the balance between the frequency and severity of losses. With all organizations being targeted, loss ratios spiked and forced wholesale corrections across pricing, retentions, coverage, and underwriting strategy.
- Organizations now faced challenges obtaining insurance and were forced to pay sharp premium increases within a tough economic climate, as well as invest in risk mitigation technologies to meet underwriter requirements.

3) **Cyber Insurance Today**

- The corrections introduced by insurers have established a new baseline for underwriting that serves to preserve the market.
- It has created new opportunities to add value through pre-incident risk management services, which should result in better risk and improved underwriting performance.

What are cyber insurance policies being bought by Canadian organisations?*

30% purchase a cyber insurance add-on. [13]

29% purchase cyber insurance policies [13]

17% do not purchase cyber insurance. [13]

25% do not know / prefer not to say. [13]

There is still a lot of growth potential in the Canadian cyber insurance market, with the majority of organizations not having yet purchased a dedicated cyber insurance policy.

Being able to explain cyber threats and the value of cyber insurance to an organization presents an opportunity for brokers to grow their portfolio, while ensuring better protection for their clients.

* Figures shown based on a CIRA survey following 510 cyber security decision makers (*i.e.: employees or owners responsible for cyber security within their organization*). While not captured in the survey, it is understood that SMEs typically lean towards add-on cyber coverage rather than standalone cyber policies. However, as we'll cover in *Section 3*, it is important for brokers to review coverage with their clients to ensure that they have adequate coverage.

Click on each underlined element to be directed to a slide providing further details

Section 2 - References

P. 16	[1] MSA research data
P. 17	[2] Josephine Wolff, ***Cyber Insurance Policy***, 2022 [3] KPMG Market Study, 2023 [4] Ruperto P. Majuca, William Yurcik, Jay P. Kesan, ***The evolution of Cyber Insurance***, 2006
P. 18	[5] Josephine Wolff, ***Cyber Insurance Policy***, 2022 [6] The New York Times, ***The Ashley Madison Data Dump, Explained***, 2015 [7] KPMG market study, 2023
P. 19	[8] Forbes, ***The Rise Of Targeted Ransomware Attacks***, 2019 [9] Canadian Underwriter, ***How much Canadian insurers have lost on cyber liability so far in 2021***, 2021 [10] Coveware, ***Quarterly Ransomware Report, Q2 2022***.2022
P. 20	[11] KPMG market study, 2023 [12] Newswire, ***Cyber insurtech BOXX Insurance announces USD $10M Series A round to further accelerate growth, prepare for international expansion***, 2021
P. 21	[13] Canadian Internet Registration Authority (CIRA), ***Cybersecurity insurance popular in Canada despite imperfections,*** 2021

Section 3

Empowering Brokers to Better Serve Their Clients

Overview: Empowering Brokers to Serve their Clients Better

Now that you understand the cyber insurance market from both the point of view of cybersecurity and of underwriters, it is important to ask **how can brokers stand out within the market, and better serve their clients?**

Key topics and questions addressed in this section:

1) **Opportunities and Challenges: Key Trends**
   - Key trends affecting the cyber insurance market.
   - Challenges and opportunities for brokers.
   - What are clients looking for?
2) **Target Policy Cycle**
   - An overview of the cyber insurance placement process.
   - Guiding questions for enhancing each step of the policy lifecycle.
3) **Initial Consultation & Insurance Readiness Assessment**
   - Why does my client need cyber insurance?
   - Using the initial consultation to identify the right clients.
   - How can I get the best quote possible for my client?
4) **Application Process**
   - Understanding minimum controls and requirements.
   - Understanding evolving insurer risk appetites.
5) **Quote Bind, Onboarding, Collection, and Analysis**
   - What you should be aware of – exclusions & conditions, first & third party coverage, and services.
   - What to look for when choosing policy terms.
6) **Claims Management**
   - Faster is cheaper – Clients need to be ready to face a cyber incident.
7) **Mid-Term Contact**
   - Tools and partners – how can brokers add value?

Clients expect their brokers to have…

Cyber insurance knowledge

Expertise in cybersecurity

Which means brokers need to…

1. Be well versed in policy coverages, triggers, conditions and exceptions
2. Have tools that streamline the application process
3. Understand minimum control requirements

Click on each underlined element to be directed to a slide providing further details

Key Trends, Opportunities, & Challenges for Brokers

Changes in **demand, capacity, price competition, coverage options,** and **underwriting risk assessment present challenges and opportunities** for brokers seeking to go beyond traditional practices to become a trusted cyber risk manager for their clients.

Key Trends

Increase in demand: With a complex threat landscape (Section 1) and increasing customer awareness, the demand for cyber insurance, particularly standalone, will continue to grow.

Tighter underwriting measures: To prevent cyber incidents, insurers will rely on technical risk assessments, increasing the burden of proof required for customers to obtain favorable insurance terms.

Enhanced coverage options: Insurers are refining their coverage to be more tailored and comprehensive (*e.g. specific to different industries, improved terms, coverage enhancements for emerging risks*). Standalone policies will grow in popularity.

Changes to premiums: As the market softens, increasing competition will put downward pressure on premiums. Improvements in risk assessment will result in better T&C's for customers with best-in-class underwriting submissions.

Challenges For Brokers

- **Lack of standardization:** underwriting appetite and application minimum controls vary between carriers, requiring brokers to prepare clients for a broad range of expectations at market.
- **Skills gap:** technical conversations require brokers to invest in the knowledge and skills required to provide advisory services to clients, and to support them during negotiations with underwriters.
- **Policy lifecycle intervention:** success in the market requires intervention throughout the policy lifecycle, demanding time and resources from brokers to ensure clients meet market standards.
- **Risk of destabilization:** the long-term stability of the market will depend on brokers who recognize the value of technical underwriting and are cautious of markets taking a softer approach.
- **Legislation and regulations:** provincial and federal regulators are enhancing the safety and privacy of data that could result in a changing loss environment and new minimum controls.

Opportunities For Brokers

- **Cyber risk management program:** the lack of standardization reflects the complex nature of managing cyber risk, which ensures that brokers are valued as cyber risk management advisors.
- **Frequent client engagement:** the role of the broker throughout the policy lifecycle offers new scope for value-add services and enhancing client relationships.
- **Investment in skills:** investing in the knowledge and skills needed to become a trusted cyber risk advisor to clients can lead to a reputation among clients that drives portfolio growth and retention.
- **New revenue streams:** as a cyber risk advisor, services that can be offered through commission fees and other value-add services present opportunities for new revenue growth.
- **Softening market:** as a result of improving loss ratios, increasing capacity and competition offers brokers the scope to re-negotiate pricing and grow towers with new excess layers available.

Takeaway

- Current trends within the cyber insurance market present both **challenges and opportunities** to insurance brokers seeking to **grow their status as a trusted cyber risk management partner** for their portfolio of clients.
- A window of **opportunity exists for brokerages willing to grow their understanding of cyber risk management** through both transfer and mitigation, to become market leaders in cyber risk management services.

What Are Clients Looking For?

To be effective at selling cyber insurance, brokers need to understand that **clients require more than just an insurance broker**. Clients need a **risk management advisor** capable of combining risk transfer (cyber insurance) with risk mitigation to enable their overall strategy.

What is Important When Choosing a Cyber Insurance Broker?

Cyber insurance knowledge

To be effective in this market, brokers need to understand:

- Underwriter appetite.
- Common minimum controls required by insurers.
- Common coverages and restrictions, and their relative impact across various industries.
- Pre- and post-breach services.

This is due to the following elements, which make cyber insurance different from other Commercial and Speciality Lines:

- High variability of wordings used across different insurers.
- Different underwriting requirements for different organisations and industries.

Clients need a broker who can accompany them through choosing the right cyber security coverage and services to suit their risk appetite and address their loss concerns. Clients value the ability to articulate how coverage will be triggered in a loss scenario, its relevance to the incident experience of a client in any industry, as well as the benefit of cybersecurity controls required to be insurable.

Expertise in cybersecurity

To be effective in this market, brokers need to understand:

- Why are organizations at risk, even with best-in-class controls?
- How are different industries targeted and impacted by threat actors?

When selling cyber insurance, brokers will usually deal with different stakeholders, including CISOs and IT managers – however, there are instances in which SMEs do not have in-house expertise, and instead have to outsource such work. This is a significant challenge for brokers.

A cyber insurance broker must act as a trusted advisor to such stakeholders when it comes to cyber risk management. They need to:

- Advise on risk management strategy (*e.g.: vulnerability prevention roadmap development, prioritization*). This requires brokers to educate themselves in risk management practices.
- Find 3rd party solutions to assist clients with the implementation of their roadmap to achieve insurability.
- Understand and explain the value of risk management controls, including compensating controls, to both clients and underwriters during planning and negotiations.

Takeaway

- A key difference with ‘traditional’ insurance markets (CGL, D&O, etc.) is that **brokers are seen as cyber risk management advisors.**
- However, similarities between the **skills brokers need for success in other product lines — such as communication, sales, relationship building, problem-solving, and analytical abilities** — make the cyber insurance market accessible even for brokers who may not be experts in cyber.

Target Policy Cycle

The cyber insurance policy lifecycle covers five different steps, each of which represent an **opportunity for brokers to intervene and provide value-added services for their clients**.

After this section, you will be able to address the following questions across the cyber insurance policy lifecycle

01. Initial Consultation & Insurance Readiness Assessment

- What are the client's specific needs (coverage, regulations particularities, etc.)?
- What are the client's current cybersecurity measures, risk exposure, and vulnerabilities?

03. Quote Bind, Onboarding, Collection, & Analysis

- What are the key coverages and pre/post breach services that the clients require?
- What conditions must clients be aware of?
- What onboarding process do clients go through?

05. Mid-term Contact

- Which cyber risk management practices need to be re-examined to ensure better policy pricing?
- What new market conditions, trends, vulnerabilities, or threat actors does the client need to be made aware of?

02. Application Process

- How can the application process for different insurers be streamlined to ensure optimal client experience?
- What additional information can be shared to enhance the risk profile of the client beyond "tick box" questions?

04. Claims Management Process

- How can brokers intervene to improve the claims process?
- Who can brokers work with to facilitate a claims evaluation?
- What cyber risk management practices do brokers need to be aware of to efficiently prepare for a post-incident review?

Why does my client need cyber insurance?

Similar to most insurance products, clients derive value from brokers through their **identification of coverage tailored to their needs**.

Why do clients need cyber insurance?

Guiding questions to help you assess these needs

1. High exposure to cyber threats	• Does the client rely on the availability of IT Systems or information stored and processed by systems for its business operations? • What impacts have cyber attacks had on comparable organizations?
2. Need for pre- and post-breach services	• Does the client possess the necessary expertise to effectively navigate a cyber incident? • Would the client benefit from gaining access to Insurance Panel service providers? • Does the client have existing service providers on retainer?
3. Financial security	• Does the client's organization have strong liquidity to manage the costs of a cyber incident? • Are they able to take on larger retentions to manage premiums?

Despite the complexity of cyber security, brokers need to demonstrate the value provided by cyber insurance.

Common misconceptions and objections

"My business is too small to be targeted by cyber attacks."	The frequency of cyber attacks against SMEs is higher than for larger organisations, which presents an easy target and a return on investment for financially motivated threat actors.
"My IT service is top quality, meaning I don't have any cyber risks."	Cyber incidents caused by human error (80%+) combined with a threat landscape that enables residual risk makes it impossible for IT services to guarantee the prevention of cyber threats.
"I already have an add-on to my commercial insurance, why pay more for a standalone policy?"	The costs of managing a cyber incident and the value provided by comprehensive coverage and services available through a standalone policy is necessary for peace of mind in a time of crisis.
"Cyber Insurance does not typically pay claims."	Loss ratios experienced by the market prove otherwise – insurance carriers have paid claims, leading to today's market conditions.

Takeaway

- Similarly to other insurance products, common objections usually derive from a false perception of cyber risk. **Most, if not all SMEs would benefit from having a solid cyber insurance policy**, both from a risk management perspective, and through deriving value from complementary services.

01

Different Industries, Different Threats, and Different Needs

A few basic concepts can be used to **identify the specific needs of different clients across various industries.**

Which activities of business processes in various industries would heavily impact organizations if interrupted?

Transport & Logistics				
Order Management	Inventory Management	Fleet Management	Freight Forwarding	Route Optimisation
Retail				
Vendor Management	Inventory Control	Point of Sale (POS)	E-Commerce sales	Customer Service
Manufacturing				
Production Scheduling	Quality Control	Supply Chain	Maintenance Scheduling	Post-sales Support

Examples of cyber attacks and their impact on different industries

Distributed Denial of Service (DDoS)
Inundation of online resources with malicious traffic, causing prolonged downtime or forcing them to shut down.

Web application failures caused by a DDoS attack can lead to the shutting down of fleet management systems, creating delays in orders, communications breakdowns, and severe impacts on revenue generation and customer satisfaction.

Example [1] **:** in 2012, a DDoS attack on the Québec government's portal website caused it to shutdown, rendering it inaccessible for over two days.

Ransomware Encryption of critical data to render it unusable, followed by ransom demand. Risk of losing data permanently if decryption fails.

A ransomware attack targeting a POS system can cripple operations by encrypting transaction data and rendering the POS inoperable. This results in revenue loss, customer dissatisfaction, and potential regulatory consequences.

Example [2] **:** in 2022, a mining company based in British Columbia was hit by a ransomware attack, forcing them to shut down their mill and lose their production.

Social engineering and fraudulent emails
Impersonation of trusted entities to deceive employees into divulging confidential data, transferring funds, or sharing login credentials.

A social engineering attack through an email pretending to come from a trusted supplier can lead to disrupted deliveries and vendor relationships, resulting in delayed shipments, financial losses, and reputational damage.

Example [3] **:** in 2021, Canada Post was hit by an attack through a third party vendor. Postal addresses and contact information were exposed, affecting 950k parcels.

Takeaway

- Different industries face **different types of cyber risk, and benefit differently from different cyber insurance coverages.**
- Organizations expect a certain level of customization to their cyber insurance policy. As such, it is important for **brokers to be able to understand the specific risk management needs of their clients.**

How Can I Get the Best Quote Possible for my Client?

To be considered for cyber insurance, **organizations need to meet certain minimum controls** (specified within the following pages). Cyber insurers are focusing more than ever on prevention of cyber risks, and partner with organizations proactively managing this risk.

Is my client insurable?

Insurers typically set specific requirements, or 'minimum controls,' that an organization must implement to be eligible for coverage.

These controls serve as essential safeguards to reduce the insurer's risk.

Minimum controls vary between insurance providers

While several common requirements exist, the required controls vary across insurers. Even offers from a single provider can vary between industries.

However, remember that insurers **offer more favorable coverage terms and premiums to businesses that have strong cybersecurity practices.**

How can I help my client build a simple roadmap to address these gaps?

1. **Understand the market appetite:** Build an assessment to identify any potential road-blockers in the client's risk profile that will impact their opportunity of obtaining a cyber insurance policy. Enhance the assessment to include controls from industry frameworks such as National Institute of Standards and Technology (NIST) Cybersecurity Framework to ensure clients are staying ahead of changing market conditions.
2. **Involve key stakeholders:** Cyber insurance requires the engagement of stakeholders from across the business, not just those involved in risk management. Any IT security roadmap will typically be owned by CISOs or their equivalent - their involvement in triggering the policy in an incident scenario is required, so it is important for them to be involved in key decisions.
3. **Complete the assessment:** Coach the client through completion of the assessment, and identify compensating controls to fine tune remaining gaps against underwriting appetite and industry control requirements.
4. **Create the roadmap:** Use assessment findings to develop a prioritized list of controls to be implemented. Identify which controls are required before approaching underwriters, and which can be worked on after the policy is bound.
5. **Offer solutions to achieve insurability:** Work with vendors or develop in-house capabilities to offer solutions to clients that will enable the implementation of roadmaps. Prioritize solutions which will address minimum controls demanded by underwriters.
6. **Review iteratively:** follow the roadmap's progress, making adjustments as needed to address emerging threats and changes in the organization's risk profile.

Takeaway

- Consolidate the minimum control requirements from key markets to **build a single assessment questionnaire** that can be used to determine whether a client is insurable, and what measures must be taken to make them insurable if necessary.
- Ensure that **relevant stakeholders are involved in cyber insurance conversations**, to improve information gathering during assessments and ensure buy in for roadmaps and other conditions necessary, maximizing the value of cyber insurance.

Understanding Minimum Controls & Requirements (1/3)

There are **several frameworks** which brokers and clients can use to **inform their cyber risk management strategies**. By managing cyber risk through a layered approach capable of navigating a threat at each step of the attack kill chain, organizations will be best placed to obtain insurance, mitigate severity losses, and be an asset to the broker's portfolio long-term.

People, Processes, and Technology must work in sync, enabling a holistic approach to cyber risk management

People
Personnel capable of supporting a cybersecurity program, and skill shortages which must be addressed via hiring or outsourcing.

Processes
Critical business processes which generate revenue, support the wellbeing of personnel, and deliver other business functions on a day to day basis.

Technology
Critical and sensitive IT assets which are utilized by business processes, and well as have access to sensitive information.

The kill chain of a ransomware attack is composed of 5 distinct steps – each requiring control capabilities that align with the NIST CSF to manage threats, demonstrating the need for a well-balanced cybersecurity program.

01 **Reconnaissance**: Threat actors find and leverage publicly available information, to gain insight to the organization's attack surface and inform social engineering efforts.

02 **Gain Access**: threat actors seek to gain access by identifying vulnerabilities and weaknesses in exposed services.

03 **Establishing Persistence**: Once inside, threat actors seek to expand their access levels, moving laterally and deploying remote access tools (RATs) to cement a persistent foothold in the target network.

04 **Compromise and Escalation**: Ransomware requires administrative access to the most sensitive parts of the network to remove any chance of the organization not paying the ransom. Escalation of privileges is the next target for threat actors, to gain the keys to the kingdom.

05 **Achieve Objectives**: Having gained sufficient administrative privileges and access to critical systems, databases, and backup servers, the threat actor is ready to detonate the ransomware.

Identify: An organization must know what its assets are, and the value of those assets, to inform the application of controls and cyber risk management decisions.

Prevent: The 1st step in cybersecurity is reducing the likelihood of an incident occurring, which requires a risk-based approach informed by cyber threat intelligence. Prevention controls must be implemented on external facing assets, end user workstations, and servers to deter threat actors gaining initial access.

Detect: Incidents will happen; an organization's ability to monitor for and rapidly detect anomalies early on in the threat actor's kill chain will mitigate the most severe impacts an organization may face.

Respond / Recover: Having declared an incident, hopefully in its infancy, the business must contain and eradicate the threat before restoring systems back to functionality. In this high stress crisis environment, being ready can mitigate the loss further by enabling the organization to return to business as usual operations as the earliest point possible.

Understanding Minimum Controls & Requirements (2/3)

Understanding the **minimum controls and requirements** for cyber insurance is rendered easier for organizations by **sorting their critical and sensitive assets, as well as the kill chain phase they are most at risk for, into larger frameworks** – this simplifies **cyber risk management strategizing** and the cyber insurance **application questionnaire process**.

	Control [4]	NIST CSF	Explanation
People	**Incident Response Planning and Testing**	**Identify** **Respond & Recover**	It is vital that **all responsible parties understand their role** in responding and recovering from major incidents. Regular tabletop exercises involving internal and external stakeholders improves response plans before crises occur.
People	**Awareness Training and Phishing Exercises**	**Prevent** **Detect**	Awareness training provides users with the **knowledge and skills to navigate their roles and responsibilities securely**, while phishing exercises and other simulations create a **safe environment for users to apply that training**.
Process	**Secured, Encrypted, and Tested Backups**	**Respond & Recover**	An organization's ability to recover mitigates the extent of a loss. When backups are accessed by the threat actor, clients are often forced to pay a ransom. Ensuring that backups are stored within **secure segments that are disconnected from Active Directories** (for which credentials are tightly controlled), and 'immutable' where possible, protects them from unauthorized tampering. Clients must also recognize that while forensic investigations are ongoing, their ability to restore backups to production servers could be impacted. This delay will cost them money, so having **redundant hardware is vital for a rapid recovery during investigations**.
Process	**Privileged Access Management (PAM)**	**Prevent** **Detect**	PAM is the process of managing both human and non-human privileged access. PAM involves **implementing least privilege principles to reduce the number of accounts with 'keys to the kingdom', and the ability for threat actors to escalate privileges.** PAM tools also assist organizations to **manage account credentials** (including rotation & update practices), as well as tracking identifies to **monitor and analyze activity to detect threats**.
Process	**Patch and Vulnerability Management**	**Detect** **Prevent**	Robust vulnerability management programs assist organizations to **identify critical & high severity vulnerabilities and patch them swiftly,** to reduce an organization's attack surface and prevent known vulnerability exploitation.
Process	**Hardening Techniques and Configuration Management**	**Prevent**	IT systems often come with default settings and administrator accounts, increasing attack surfaces. CIS benchmarks provide **secure configurations to manage IT Systems**, reducing unnecessary services and exploitable vulnerabilities. Baseline configuration compliance must be managed as a high priority security process.

Understanding Minimum Controls & Requirements (3/3)

Understanding the **minimum controls and requirements** for cyber insurance is rendered easier for organizations by **sorting their critical and sensitive assets, as well as the kill chain phase they are most at risk for, into larger frameworks** – this simplifies **cyber risk management strategizing** and the cyber insurance **application questionnaire process**.

	Control [4]	NIST CSF	Explanation
Technology	**Asset inventory**	**Identify**	Maintaining an asset inventory, that lists IT assets according to sensitivity and criticality, is vital in assisting an organization to **apply preventative controls**, as well as to assist **prioritize the recovery of assets** following a major incident.
	Email Filtering and Web security	**Prevent**	Email filtering technology **blocks suspicious emails, identifies hidden malware, and detonates attachments & links** before users receive messages. Web security protects users browsing the internet, **blocking known malicious websites and preventing downloads that contain malware**.
	Logging and Monitoring Network Protections	**Detect** **Response & Recover**	The ability to identify, detect, and respond to cyber threats lies in an organization's ability to **aggregate and analyze logs generated across a network**. SIEM solutions, integrated with all systems in use and supported by a SOC monitored 24/7, will enable early detection and loss mitigation through quick response.
	MFA – All Remote Access	**Prevent** **Detect**	MFA must be in place for all remote access to prevent threat actors from using stolen credentials to access environments. Underwriters also want MFA in place for on premise privileged access.
	Endpoint Detection and Response (EDR)	**Prevent** **Detect** **Response & Recover**	EDR tools can be configured to block anomalies (*e.g.: attempt to access a workstation from a suspicious location, or at a time diverging from user behavior patterns*). EDR tools also have the ability to contain incidents early, preventing lateral movement. All workstations and servers should have EDR at minimum.

Takeaway

- The minimum controls and requirements that fall within the **Prevent and Response & Recovery steps of the NIST framework are the most prevalent** – these steps focus on minimizing the impacts of an incident and providing organizations with resiliency against cyber threats.
- Cyber risk is complex, made evident by the lack of standardization in underwriting appetite. Brokers must guide clients to implement and value controls **across all 5 pillars**, to ensure that they are capable of managing each step of a kill chain and to maintain a client's insurability status**.**

What You Should Be Aware Of – Exclusions And Conditions

Brokers need to be aware of **common conditions and exclusions** which may have important impacts on the value provided by the policy.

Common Policy Triggers

Data Breach
Unauthorized access to company data.

Security Breach
Failure of computer security to prevent unauthorized access to company IT and information assets.

System Failure
Unintentional or unplanned outage to a computer system, without malicious intent.

What Common Conditions Should Brokers Be Aware Of?

Ransomware co-insurance: Co-insurance is used to manage significant risks with insufficient minimum controls. Clients are consequently responsible for 50% of the loss resulting from ransomware in addition to the policy retention. It devalues the policy from a financial indemnification perspective. Brokers can drive organizations to enhance their insurability by improving controls.

Condition precedent wording: Condition precedent wordings require clients to meet certain conditions for coverage to apply (*e.g.: system neglect endorsement reduces coverage for losses resulting from an unpatched or end-of-life system*). It highlights the connection between cyber risk management and cyber insurance, and the need for brokers to ensure that clients have appropriate procedures in place to maximize the value of their policy.

Notification clauses: Notification clauses serve to inform insurers of cyber incidents in a timely manner, enabling them to mitigate losses quickly and prevent threat actors from progressing through different kill chain phases by activating breach response vendors. Insureds are required to notify their carrier as soon as reasonably practicable upon discovery of an actual of suspected incident that triggers the policy. Failure to do so may result in losing coverage for the resulting claim.

Period of indemnification: A period of indemnification determines the time period in which losses can be calculated for business interruption. Some periods begin from the moment of interruption, with coverage triggered following the lapse of the waiting period. Others begin after the waiting period has elapsed, leaving a period of loss not covered.

Claims aggregation: Cyber insurance policies may contain aggregation language, treating related or similar claims as one. This minimizes insurer exposure, so that the total indemnification does not exceed the agreed per-claim limit. However, this can also benefit the insured if they can pool together several smaller losses so that the overall amount exceeds the retention and triggers the liability of insurers. Wordings need to be carefully considered for any ambiguity in interpretation.

What Common Exclusions Should Brokers Be Aware Of?

War exclusion: In the absence of the state declaring that a cyber attack originated from an aggressor state, and thus declaring cyber war, the war exclusion recently released by Lloyd's of London can only be used in the event that a nation state is unable to administer critical services, such as healthcare, utilities, and financial services. turning a nation state into an "impacted state." Clients should feel confident that an attack that impacts their organization, in an isolated or non-systemic event, will be covered.

Infrastructure exclusion: Infrastructure exclusion is common in policies across all lines of business. Although it remains independent to the war exclusion, concerns over aggregated cyber risk mean that policies invariably exclude losses arising from the failure of utilities (*e.g.: electricity, gas, water*), internet service providers, telecommunications, and satellites.

Takeaway

- Clients need to **be aware of the triggers, conditions, and exclusions of their specific policy**. An in-depth discussion about these subjects will save a lot of effort and will help the **client be ready in case of a claim.**

What You Should Be Aware Of – First Party Coverage (1/2)

Indemnification provides financial compensation following cyber attacks – it is commonly **split into 1st and 3rd party coverage**. However, **variability in policy terms, nuances in exclusions, and coverage** make the cyber insurance landscape **difficult to navigate**. Keep in mind certain fine and penalties resulting from incidents may not be insurable by law, if they are punitive due to gross misconduct.

First Party Coverage provides protection for an insured entity against direct losses and damages to their own property or assets.

Coverage Type	Definitions	What you should be aware of… [5]
First Party Data Breach	Coverage for costs associated with responding to a data breach. Examples include: legal and PR expenses, forensic investigation expenses, and credit monitoring costs.	Many insurers have strict requirements for clients to use panel vendors they provide. Some markets offer "limit in addition", increasing the additional coverage for relevant costs. • **Benefits**: organizations can leverage vendor experience and expertise during incident response, as well as enjoy preferential rates. They receive additional limit above the overall aggregate limit to pay for notification and incident response costs during a data breach. • **Drawbacks**: if a client has an existing IR retainer, they no longer have the flexibility to use their own vendors.
Network Business Interruption (BI)	BI provides coverage for lost income, business continuity, or disaster recovery expenses incurred during network downtime as a result of a security failure or system failure.	Calculating BI losses is achieved through using assumptions based on data from previous years, as well as current performance trends – this serves to identify direct revenue loss as a result of a disruption. • **Benefits**: BI loss calculations are useful for organizations that sell products or goods, as direct revenue from sales is easily assumed. If an organization's client moves their business elsewhere as a consequence to BI, reputational loss coverage may also apply. • **Drawbacks**: Organizations need to understand how BI loss is calculated for their specific business to have a realistic expectation for coverage (e.g.: lost revenue for contract or service-based organizations is usually difficult to quantify, making the final amount highly contestable on the insurer end).
Dependent Business Interruption (DBI)	DBI refers to the insured's loss of income resulting from a third party service provider's own security or system failure.	A challenge within DBI is defining what counts as a dependent business. Requirements for a business to be considered as such usually include having a direct relationship with the organizations and a contract in place. **Particularities**: • Some markets differentiate between IT and non-IT vendors. • Losses due to an impact caused by a vendors of a vendor will not be covered.

Takeaway

- The minimum controls and requirements that fall within the **Prevent** and **Response & Recovery** steps of the NIST cybersecurity framework are the most prevalent – these steps focus on minimizing cyber risk, and oftentimes leveraging panel vendor relationships to mitigate risk.
- While controls falling within the Prevent NISF step focus on minimizing cyber risks, ensuring that controls and requirements corresponding to the **Identification and Detection steps would encourage stronger risk management and mitigation** within client organizations.

What You Should Be Aware Of – First Party Coverage (2/2)

First Party Coverage provides protection for an insured entity against direct losses and damages to their own property or assets. [1]

Coverage Type	Definitions	What you should be aware of… [5]
Reputational Loss	**Reputational Loss** provides coverage for lost profits associated with the loss of current or future customers due to reputational damage resulting from a cobered	**Particularities**: • Certain policies are only triggered if the incident become a pubic media event - if the media do not publicly declare the incident, coverage would not apply. • Lost profits are sometimes covered only if they were incurred during a "reputational harm period," a designated window of time following discovery of the cyber event.
Cyber Extortion & Cyber Crime	**Cyber Extortion** provides coverage for expenses resulting from a cyber extortion incident or attempt (e.g.: support services to inform decision makers, funding available for aiding in payment for ransoms where legally applicable). **Cyber Crime** provides coverage for losses resulting from social engineering scams (e.g.: fraudulent fund transfers and/or transactions).	**Cyber Extortion Particularities:** • Certain insurers will require organizations to provide Verification of Extortion, which ensures that a credible threat or actual extortion attempt has taken place before a claim can be filed. • Cyber Extortion clauses may sometimes only cover the cost associated with a ransom payment, excluding damages and losses incurred from lost income, costs, or BI. **Cyber Crime Particularities:** • Social engineering attacks are widely considered a gray area, and include loopholes for Insurers to deny coverage (e.g.: employee voluntarily transfers money on behalf of the company, fraudulent requests being completed over the phone rather than computer).
Data Recovery Costs	DRC provides coverage for costs incurred to restore or re-build data following a cyber security incident.	**Particularities:** • Language often reads as "to replace, recreate, restore, or repair programs, software, or data." Restoring data from backups remains the best option for clients – to recreate or replace data is challenging, time consuming, or impossible depending on the industry. • Brokers must ensure that clients understand the realities of this process, and ensure that backup and recovery processes are thorough.

Takeaway

- *Reminder*: Clients want a **broker who will be able to advise them**, on the best coverage to help their specific needs.
- An in-depth **understanding on how the different coverages damages are calculated** will allow you to better advise clients. Remember that limits and nuances vary a lot between underwriters.

What You Should Be Aware Of – Third Party Coverage

Indemnification provides most of financial compensation following cyber attacks – it is commonly **split into 1st and 3rd party coverage**. However, **variability in policy terms, nuances in exclusions, and coverage** make the cyber insurance landscape **difficult to navigate**. Keep in mind certain fine and penalties resulting from incidents may not be insurable by law, if they are punitive due to gross misconduct.

THIRD PARTY COVERAGE protects businesses against claims and legal expenses arising from third party lawsuits related to data breaches, privacy violations, and network security failures. [6]

Privacy Liability : policies provide protection against financial losses and legal expenses resulting from claims related to the mishandling, unauthorized access, or inadvertent exposure of individuals' private and sensitive information in the event of a data breach or cyber incident.
Examples of damages covered – legal fees, settlements, or regulatory fines.

Multimedia Liability : policies provide protection against financial liabilities resulting from legal claims related to the creation, publication of distribution of multimedia content that allegedly cause harm, infringement, or defamation to third parties. In an era where content creation and dissemination occur across various digital platforms, this coverage is increasingly important for businesses to adequately protect themselves online.
Examples of damages covered – intellectual property rights, copyright infringements, or reputational harm to a third party.

Regulatory and Legal Support : policies provide assistance in managing the financial burdens arising from regulatory inquiries, legal actions, and associated costs stemming from data breaches or cyber incidents affecting external parties. Given increasing stringency and diversity of data protection regulations, this coverage is instrumental in ensuring that organizations can adeptly address legal and regulatory challenges that emerge post-cyber incidents.
Examples of damages covered – legal fees, compliance-related costs, or fines imposed by regulatory authorities.

Network Security and Privacy Liability : policies provide essential protection against financial liabilities resulting from legal claims initiated by external parties due to data breaches or cyber incidents resulting from an organization's inadequate network security or breach of privacy. This includes errors, omissions, or negligence by the insured following a cyber event.
Examples of coverage –legal actions, settlements, and damages claimed by affected third party.

Common Triggers [7]

Claims alleging a breach of confidential data, confidential corporate information.

Claims made after suffering a loss occasioned by an insured's lack of cyber security (e.g.: the inadvertent transmission of malware).

Claims by the insured when a 3rd party IT outage occurs (often known as an outsource service provider or contingent business interruption cover).

Takeaway

- Triggers for third party coverages differ form the ones present in first party coverages. As such, some organizations should put their focus on increasing their third party coverage limits while others should focus on first party. **Think back on what type of threat and on what part of their business process, a cyber attack could have the biggest impact.**

Cyber Insurance & Services – Policy Term Glossary

Cyber insurance's evolution challenges the classic indemnification insurance model, as the industry takes strides towards becoming **increasingly service-based**. For SMEs, the benefits derived from these **services represent the real value-add** from cyber insurance.

PRE-INCIDENT SERVICES

help policyholders manage cyber risks before an incident occurs, enhancing cybersecurity posture and reducing the likelihood of a cyber attack. [8]

Cyber Risk Assessment & Vulnerability Scanning: policies include services that assess cyber risk profiles, identifying vulnerabilities within current cybersecurity practices and systems. Guidance is provided to enable timely remediation, implement cybersecurity measures to mitigate risks, and inform various internal decisions.

Security Consulting: policies provide access to cybersecurity experts or consultants who can provide guidance and advice on strengthening security measures. Professionals may assist in developing cybersecurity policies, implementing best practices, or conducting employee training programs.

Incident Response Planning: policies are set to provide assistance in creating or improving an incident response plan tailored to the policyholder's specific needs. This plan outlines steps to be taken by SMEs in the event of a cyber incident, ensuring a timely and coordinated response to minimize damage and facilitate recovery.

Legal and Regulatory Compliance Support: policies include legal, privacy regulations, and industry or province-specific compliance regulations (data breach notification requirements vary across Canada). This helps ensure the policyholder's cybersecurity practices align with legal obligations, reducing the risk of potential penalties or fines.

POST-INCIDENT SERVICES

help policyholders manage and recover from a cyber incident, minimize impact, facilitate recovery, and ensure that normal operations can resume in a timely manner. [9]

Incident Response Coordination: policies assist coordinating the response to a cyber incident, usually with teams of experts guiding and supporting policyholders through the response process (*e.g.: incident containment, evidence preservation, and collaboration with law enforcement*).

IT Forensic Investigations: policies provide forensic investigation services. Services aim to determine the cause and extent of the cyber incident, identify compromised systems or data, gather evidence for potential legal proceedings, and sometimes provide comprehensive reports on the incident.

Data Breach Response Panels: policies help businesses navigate data breach notification requirements through legal compliance with province-specific regulations, assessment of notification obligations & expenses, and assistance in distribution of breach notifications to affected parties.

Public Relations & Reputation Management: policies assist with public relations and reputational impacts of a cyber incident, covering expenses and directing businesses to PR consultants & crisis management services, and facilitating communication efforts to mitigate reputational damage.

Legal Support & Regulatory Compliance: policies help SMEs navigate a cyber incident's legal implications (*e.g.: provincial regulatory requirements*).

Takeaway

- **Cyber services are highly valued by SMEs**, as they might **not have the capacity for or expertise in** cyber risk management and response.
- Due to the high variability in cyber exposure, **quantifying the cost of a data breach is challenging** and makes planning for risk management, remediation, and the amount of coverage to request from insurers difficult.
- The rise of Insurtechs and various technological advancements create an unprecedented opportunity for brokers to **differentiate themselves.**

An Easy Way to Compare Quotes

Similarly to other products, clients look for brokers who are able to make the process of picking their new insurance policy **simple and convenient.** Clients seek brokers who are able to **cut through the complexities of their options when communicating.**

Brokers should leverage a quote comparison template to…

Create a side-by-side view to compare key terms and conditions across quotes.

Streamline the process in reviewing the quote comparison process, while reducing potential errors & omissions exposure in review.

Develop a template that can be used to present to the client.

Example of a Quote Comparison Template - Illustrative

		Quote #1 - Insurer A	Quote #2 – Insurer B	Quote #3 – Insurer C
GENERAL	Package vs Add-On			
	Premium			
	Aggregate Limits			
FIRST PARTY COVERAGE	First Party Data Breach Expenses			
	Network Business Interruption (BI)			
	Dependent Business Interruption (DBI)			
	Cyber Extortion			
	Data Recovery Costs			
	Cyber Crime			
THIRD PARTY COVERAGE	Privacy Liability			
	Multimedia Liability			
	Regulatory and Legal Support			
	Network Security and Privacy Liability			
SERVICES	Pre-Incident Services			
	Post-Incident Services			

Takeaway

- You can build in-house tools that **facilitate decision making such as quote analysis templates.** These allow brokers to **streamline their processes and highlight they key differences in coverage,** allowing for a clearer decision to be taken by the clients.

When it Comes to Claims, Faster is Cheaper

Most policies **require the client to notify the insurer "as soon as reasonably practicable"** on discovery of an actual or suspected incident. In essence, insurers want to be told quickly, so that they can activate their services to contain the incident, and prevent losses.

The Role of the Broker

1. **Support** the client in quickly reacting to the cyber incident.
2. **Leverage** to the maximum the services provided by the insurer.
3. **Be an effective representation** to the insurer.

The Advantage of Cyber Insurance

Unlike traditional insurance, the dynamic and evolving nature of its underlying risk requires **continuous advisory and support, creating ongoing touchpoints with clients,** through which Brokers can **build trusted advising relationships.**

Moreover, cyber incidents, being widespread, prompt clients to **recognize the need for protection, leading to a receptive audience**.

This heightened awareness offers brokers a prime opportunity to engage clients in discussions about comprehensive cyber coverage, risk management, and incident response strategies

Breaches with identification and containment times under 200 days have **their average costs 23% lower** that those with an average time of over 200 days.

What are the best practices to reduce reaction time? [10]

1. Build security into every stage of software development and deployment, test regularly
2. Modernize data protection across hybrid cloud
3. Use security AI and automation to increase speed and accuracy
4. **Strengthen resiliency by knowing your attack surface and practicing IR**

1-3 are traditionally addressed internally by SMEs

Incident Response (IR) planning and testing is one of the top cost mitigators. Organizations with robust IR countermeasures experienced significantly lower data breach costs, reducing expenses by USD 1.49 million compared to those with inadequate measures. Additionally, these well-prepared organizations demonstrated a remarkable 54-day faster incident resolution.

Broker should support their client in planning incident response planning and testing sessions [10]

1. **Form a dedicated IR team** with the client to meet the people you would be interacting with in case of an incident,
2. **Draft IR playbooks and regularly test IR plan**s in tabletop exercises or simulated environments to help the client leverage the right post breach services.

Takeaway

- Cyber insurance offers the advantage of bringing **the broker as an advisory in risk management.**
- A strong claims management process can save a lot of money for your client. To achieve this**, brokers need to conduct regular IR sessions, and to have a great understanding of the post breach services offered by their underwriter.**

*Illustrative

Create Value by Leveraging Partners and Tools

Incorporating **cybersecurity management services and InsurTech solutions into brokers' offerings** allows for smaller brokerages with less cyber security expertise to provide value on the cyber risk management front.

Potential Partners

Managed Security Services Providers (MSSPs)

- MSSPs offer 24/7 monitoring, threat detection, and incident response expertise. This is particularly useful for SMEs who might not have a dedicated cyber security team.
- MSSPs can be valuable partners for brokers that might not have as much knowledge in cyber risk management, and have very complementary businesses to cyber insurance.

Potential Tools

Vulnerability Assessment Tools and Cyber Security Scans

- Vulnerability assessment tools provide actionable insights into clients' cyber risks, while still being usable by non experts.
- Brokers can offer vulnerability assessment reports as part of risk assessment, enhancing their advisory role and guiding clients in addressing identified vulnerabilities.
- Furthermore, these tools can be used to better prepare clients for the quote process by improving their controls, and addressing more vulnerabilities.

Cybersecurity Training Platforms

- Cybersecurity training platforms empower brokers to educate clients' employees on cyber threats and prevention.
- Since the human element is so important in cyber risk management, having the right tools to improve client employee training in a qualified, consistent and fast manner can provide significant value to clients.

Takeaway

- To both improve the different parts of the target policy cycle, to differentiate themselves, and to finds ways to shore up areas where they might have less experience, **brokers can turn to partnerships and tools.**

Takeaways: Empowering Brokers

Cyber insurance market offers **a new product for brokers to add to their offering**, while leveraging their existing skills in communication and relationship building. To be effective, brokers need to learn more about **cyber insurance coverage types and cyber management.**

Key topics and questions addressed in this section:

Question that you should answer through your Target Policy Cycle:

01. Initial Consultation & Insurance Readiness Assessment

- What are the client's specific needs (coverage, regulations particularities, etc.)?

02. Application Process

- How can the application process for different insurers be streamlined to ensure optimal client experience?

03. Quote Bind, Onboarding, Collection, & Analysis

- What are the key coverages and pre/post breach services that the clients require?

04. Claims Management Process

- How can brokers intervene to improve the claims process?

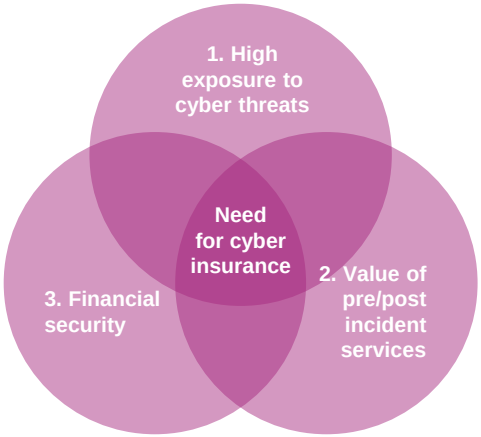
05. Mid-term Contact

- Which cyber risk management practices need to be re-examined to ensure better policy pricing ?

Key trends

- Increase in demand
- Tighter underwriting measures
- Changes to premiums

Why do clients need cyber insurance?



Streamlined processes and tools allow you to bring value in new ways compared to traditional insurance. For example:

Providing Incident Response training:

Breaches with Identification and containment times under 200 days have **their average costs 23% lower** that those with an average time of over 200 days. [10]

Click on each underlined element to be directed to a slide providing further details

Section 3 - References

P. 29	[1] RCMP, ***Cyber Crime: an overview of incidents and issues in Canada***, 2023 [2] Howard Solomon, ***Canadian copper mine hit by ransomware***, 2022 [3] Packetlabs, ***Canada Post Suffers Data Breach After Malware Supply Chain Attack***, 2021
P. 32	[4] Marsh McLennan, ***"Using data to prioritize cybersecurity investments"***, 2023
P. 33	[4] Marsh McLennan, ***"Using data to prioritize cybersecurity investments"***, 2023
P. 35	[5] One Step Secure IT, ***Cyber Liability Insurance: Here Come The Exclusions***. 2023
P. 36	[5] One Step Secure IT, ***Cyber Liability Insurance: Here Come The Exclusions***. 2023
P. 37	[6] Marianne Bonner, ***What Does Cyber Liability Insurance Cover?,*** 2021 [7] Narendran Vaideeswaran, ***Cyber Insurance Explained,*** 2022
P. 38	[8] The Balance Money, ***What does Cyber Liability Insurance Cover?*****,** 2021 [9] Woodruff Sawyer, ***Understand the Basics of Cyber Liability Insurance***, 2022
P. 40	[10] IBM Security***, Cost of a DataBreach Report 2023,*** 2023
P.42	[10] IBM Security***, Cost of a DataBreach Report 2023,*** 2023

Section 4

Appendix

Overview: Appendix

Key topics and questions addressed in this section:

1) **Result from KPMG's market study on cyber insurance**
   - Voice Of the Broker - Pain points, opportunities, and predictions for the future.
2) **Overview of Relevant Canadian Legislation Since 2019**
3) **Sample policy analysis**
   - Understanding Underwriter appetite - A CFC policy compared to a Liberty Mutual policy (*illustrative*).

Click on each underlined element to be directed to a slide providing further details

Voice of the Broker – Pain Points

We asked brokers across Canada what **challenges they experienced within the cyber insurance market**. This is what they told us:

SME Challenges

Awareness & Education : SMEs rank low in cyber risk awareness due to a lack of technical sophistication, resources, and awareness regarding cybersecurity risk management.

Security Controls & Co-Insurance : Increasingly stringent security control requirements pose challenges for SMEs in avoiding co-insurance. In most cases, insufficient controls result in restrictions and exclusions of first-party coverage.

Ransomware Payment Challenges : Loan procurement for ransomware payments is challenging due to their time-sensitive and risky nature. There is an ongoing debate regarding liability for initial payment between insured and insurer parties, although insurers are beginning to cover such payments rather than simply reimburse clients (where insurable by law, and where payments do not foul sanction laws).

Application Questionnaire Challenges : Certain clients lack the technical expertise required to complete a cyber insurance application, due to the involvement of risk management rather than IT leadership or CISOs.

Broker Challenges

Client Concerns : Basic risk management practices and an understanding of cyber insurance products are key concerns when dealing with SMEs. Some brokers are able to explore and upsell standalone packages for larger clients, but face difficulties in doing so with their SME clients.

Regulatory Compliance Challenges : Brokers are required to develop a sufficient understanding of new legislation to effectively detail and outline how controls will help clients comply with regulations.

IT Pushback & Technical Expertise : IT leadership (in particular network architects) tend to challenge the necessity of cyber insurance. Brokers should build sufficient technical expertise to navigate such discussions.

Communication & Submissions : Difficulties in contacting and receiving subsmisions from larger insurers in a timely manner have been mentioned. For brokers, it is easier to secure submissions from smaller insurers – the tradeoff when serving larger clients is that coverage may be more limited.

Insurer Challenges

Reputational Concerns : Concerns have been expressed regarding the reputational damages to the industry, stemming from lack of coverage and product quality.
Smaller insurers struggle to develop cyber products due to competition from larger insurers and InsurTechs, who benefit from technical expertise, financial capacity, and larger databases.

Market Exploration and Exit : many carriers have explored the cyber insurance market and even offered cyber products – unfortunately, many have exited due to high costs, risks, and qualifications required.

Underwriter Challenges

High Variability in Standards: Underwriting standards have been sustained, but are impacted by significant variability in wordings, requirements, nuances, and coverage provided between carriers. A desire has been expressed for standardization of application requirements, wordings, and risk profiles.
A skills gap has also come into play, as technicality and understanding of cyber insurance varies among underwriters.

Voice of the Broker – Opportunities

We asked brokers across Canada what they thought of **current opportunities within the cyber insurance market**. This is what they told us:

Rising Awareness & Education

Media Influence and Awareness : There has been a rise in cyber attacks on major players in the Banking & Financial Services industry, increasing media coverage. However, higher exposure leads to improved client awareness, which ultimately benefits the cyber insurance market.

Customized Risk and Educational Conversations : For brokers, tailoring their approach to their clients' awareness and understanding of cyber insurance is an opportunity to enhance customer experience. By being able to lead conversations regarding specific risks for each business or industry profile, brokers are personalizing their approach and increasing their impact and value-add for clients.

Internal Network Sharing : Clients are increasingly sharing access to their internal networks with brokers and underwriters in order for them to provide initial consultations and assessments of their insureability. These provide benefits for clients, helping them to avoid higher premiums and stricter policies.

Regulatory Influence on Reporting : Regulatory rigor has encouraged SMEs to report cyber attacks rather than conceal them. This opportunity for enhanced transparency and compliance benefits both insurers and the insured when it comes to data breaches and cyber incidents.

Innovation Within the Market

Rise and Prevalence of Risk Management Services : Risk management services are increasingly being offered within the cyber insurance market. They are highly valuable to SMEs:

- Cost quantifications for data breach incidents help SMEs plan for risk management, remediation, and coverage (specific to industry, organization, and PII).
- Scanning services help SMEs identify their current exposures and vulnerabilities – simultaneously reducing cyber risk, and the likelihood of higher premiums, and stricter policies before insurers complete their assessments.
- SMEs lack the capacity and knowledge to appropriately deploy Breach Response services themselves. This represents an opportunity for brokers to either develop those resources themselves, or develop relationships with service providers and experts.

Partnerships with InsurTechs and FinTechs : Collaborations with InsurTechs and FinTechs offer potential for automated distribution, provision of additional services, and access to expertise and resources. Exploring innovative partnerships for future growth represents a significant opportunity for brokers.

Voice of the Broker – Predictions for the Future

We asked brokers across Canada what their predictions were regarding **the future of the cyber insurance market**. This is what they told us:

AI Disruption & A Consequent Rise in Claims

AI disruption is predicted to increase claims due to issues surrounding privacy, data, and Intellectual Property. Current lack of maturity in understanding AI software contributes to this challenge, as this new industry continues to develop.

Trends in Pricing

Improved quality of underwriting and profitability decrease the likelihood of seeing 40-50% increases during renewals – the current situation points to a 5-15% range. Pricing in the next year will likely dictate the norm moving forward.

The Arrival of Non-Insurance Players

Non-insurance players entering the market, such as third party service providers and InsurTechs, will have significant impact. They will offer new perspectives and opportunities for innovation, while increasing competition and strain on current players.

"Race to the Bottom"

There have been mentions of concerns regarding the maintenance of market profitability, due to several elements which contribute to the "race to the bottom" dynamics. Patterns which have historically led to such situations have been observed within the market.

From Being Optional, To Becoming A Necessity

Cyber insurance is predicted to shift from being considered optional to becoming a necessity, mostly due to rising claims, growing cyber risks, and increases in general awareness. Government legislation, financial institution, or business requirements will drive this shift.

Premiums & Expansions in Coverage Provided

Premiums are not necessarily decreasing, but rather an expansion of coverage is taking place, as carriers and underwriters become more sophisticated in cyber. Insurers are now able to use granular pricing and decrease stringency of requirements, due to increasing access to data.

Overall Market Trends and Profitability

- Within the realm of brokers' experience, the **Cyber Insurance market has improved but remains unprofitable**. There are now **better controls** in terms of deductibles, competition, and the arrival of new players – these contribute to a **softening market**.
- Risks persist due to **insufficient broker and insurer education** regarding cyber security, risk management, industry differentiation, and the impact of claims.

Overview of Relevant Canadian Legislation Since 2019

Currently, **legislation relating to cyber security and privacy has been introduced at the federal level**, and both in Ontario and Quebec. Most other provinces are also considering various pieces of regulations.

Federal	**2019** - **Personal Information Protection and Electronic Documents Act (PIPEDA) amendments**. The federal government amended PIPEDA to include new mandatory breach notification requirements for organizations that collect, use, or disclose personal information in the course of commercial activities. The amendments also clarified the scope of PIPEDA to include businesses that collect, use, or disclose the personal information of their employees. **2020** - **Critical Cyber Systems Protection Act (CCSPA)**. The federal government introduced Bill C-26, the Critical Cyber Systems Protection Act, which would create a new legislative framework for protecting Canada's critical cyber systems. The bill would require organizations that operate critical cyber systems to implement appropriate security measures and to report cyber incidents to the government. **2021** - **Bill C-26, An Act Respecting Cyber Security (ARCS)**. The federal government passed Bill C-26, which amends the Telecommunications Act and enacts the Critical Cyber Systems Protection Act. The bill provides the government with new powers to mandate security measures for critical cyber systems and to respond to cyber incidents. **2022** - **Cyber Security Act**. The federal government introduced Bill C-27, the Cyber Security Act, which would create a new legislative framework for cyber security in Canada. The bill would establish a new Cyber Security Authority to oversee the implementation of the legislation and to provide guidance and support to organizations.
Ontario	**2020** - **Ontario Critical Infrastructure Cybersecurity Act**. The Ontario government passed the Ontario Critical Infrastructure Cybersecurity Act, which requires organizations that operate critical infrastructure in Ontario to implement appropriate security measures. The act also establishes a new Cyber Security Centre to provide advice and guidance to organizations on cyber security.
Québec	**2020** – **Bill 64, Law 25**. The Quebec government passed Bill 64, an act that serves to modernize legislative provisions regarding the protection of personal information. The bill includes new provisions on data breach notification, consent, and the use of personal information for advertising purposes. **2021** – **Bill 21, Ministère de la Cybersécurité et du Numérique**. The Quebec government passed an act creating the Ministry of Cybersecurity and Digital Technology, which is responsible for promoting cybersecurity and digital technology in Quebec.

Takeaway

- As of the writing of this report, **all provinces and territories in Canada had created voluntary cybersecurity guidelines for SMEs** and a detailed cyber security strategy for 2023, even if they may not have introduced specific pieces of legislation.
- Common services offered with **cyber insurance policies usually include assistance with regulatory requirements**.

Understanding Evolving Insurer Risk Appetites

It is important for brokers to understand the **risk appetite, available capacity, and services offered by insurers** to identify the most appropriate markets to engage in the application process. Below is an **illustrative view of current appetites for two insurers in Canada** (based on direct written premium). However, it is important to continue to monitor insurer appetites as they evolve.

ILLUSTRATIVE

	CFC Underwriting Ltd	Liberty Mutual Insurance
Industry Appetite	• Charities • Clubs and Societies • Entertainment & Media • Higher Education • Healthcare • Insurance Brokers • Leisure & Hotels • Logistics • Manufacturers & Wholesalers • Municipalities • Nursing Homes • Solicitors • Public Sector • Recruitment Agencies • Religious Institutions • Retailers • Support Services • Utilities • Website Operators & E-Tailers • Other Professionals	**Low Hazard:** • Business Consultants • Construction • Clubs / Associations • Cultural Institutions • Manufacturing • Natural Resources • Wholesale Distribution **Medium Hazard:** • Accounting Firms • Auto Dealers • Media & Entertainment • Personal Services • Real estate • Supply Chain / Logistics • Travel and Leisure **High Hazard:** • Government (federal) • Hospitality • Hotels • Insurance • Law firms • Technology • Wealth Management
Coverages Available	• Cyber Liability • Privacy Liability • System Business Interruption • Consequential Reputational Harm • Regulatory Actions & Investigations • System Damage • Policy Holder Privacy Breach Notification Costs • Third Party Privacy Breach Notification Costs • Cyber Crime • Multimedia Liability • Advertising Injury • Technology E&O • Court Attendance Costs • Crisis Communication Costs	• Responds anywhere in the world. • Includes full media coverage. • No exclusion for cryptocurrencies. • Full coverage for notification costs assumed by contract. • Covers punitive damages and consumer redress. • Covers breach of NDA or confidentiality agreement. • Bodily injury carve-back for mental anguish. • Trade secret carve-back.
Limits, Deductibles, Premiums	• Max. Cyber Liability Limit = $10M • Max. Privacy Liability Limit = $10M • Max. Breach Notification Limit = $5M • Max. Syst & Int. Limit = $10M • Max. Revenue = Unlimited • Min. Deductible = Nil • Min. Premium = $500	• Avail. Capacity = $10M • Target Revenue = $5M to $2.5B • Deductible Credit Available = $50K • Deductible for Breach Coach Services = $0

Takeaway

- It is **important for brokers to understand insurer's Cyber risk appetites to determine the appropriate carriers to approach** for their client. This will ensure that the client gets the appropriate coverage, while reducing time spent on completing an application for insurers who will not provide terms for the given risk.
- **Brokers must continue to monitor the evolving risk appetites of insurers, and update their assessment questionnaires appropriately.**