TELUS Business

The TELUS Canadian Cyber Insurance Study

Table of Contents

Executive summary

As the threat landscape evolves, many Canadian organizations are adopting cyber insurance to mitigate cyber risk by transferring that risk to a third party. In support of this strategy, TELUS Business has created this study to share meaningful data that identifies trends, challenges, and experiences with insurance.

Cyber insurance adoption in Canada

- Overall, **64% of Canadian organizations have cyber insurance**
- **The primary driver to purchase insurance is financial loss mitigation** stemming from revenue loss due to downtime and reputational damage
- **One in 10 organizations are considering insurance** but are still undecided
- Sixteen per cent of organizations had cyber insurance but no longer have coverage
- **One in 10 have either decided against insurance or have not considered it**

Realities of applying, qualifying for, and maintaining a policy

- As part of the application process, organizations typically had to complete one or more of the following: **an extensive security questionnaire, an internal or external vulnerability scan**, and/or a **third-party risk assessment**
- To qualify for a policy, **1 in 4 organizations had to implement or expand security processes or functions and 2 in 5 added or improved controls**
- During their last renewal, **over two-thirds of Canadian organizations received an average premium increase of 19%**
- The least likely incidents to be covered by a cyber insurance policy are **system or business failures; human error, negligence, or mistakes; and acts of war**
- **The majority of organizations (93%) are concerned about maintaining their policy coverage**

The disconnect between organizations' expectations and reality

- Almost **a third of organizations report submitting a claim** in the past 12 months
- Among those that submitted a claim, **78% received an insurance payout**, but those **payouts met expectations in only 29% of cases**
- On average, **payouts only cover 60% of incident costs**

Future improvements identified during claims process

- **Only 18% of organizations** that have experienced the claims process believe they are well protected and prepared for future incidents and claims
- Top priorities include gaining better **visibility into the attack surface**, improving **incident response plans**, and boosting **threat detection and response** measures
- **Organizations recognize they need third-party experts to help improve their security strategy and controls**, with 34% saying they need a managed security services provider (MSSP) to address control gaps and 26% looking to outside advisory services to better understand their risk

Every organization's journey will be unique

Canadian organizations face significant challenges in obtaining and maintaining cyber insurance coverage, including high premiums, compliance costs, along with the complexities of the application process. Organizations need to assess their risk tolerance to understand the types and amount of coverage they require. With this understanding, organizations can align their security measures accordingly, proactively prepare for insurance assessments, implement necessary processes and controls to address identified gaps, and invest in tools for effective response and recovery. Ultimately, organizations can consider cyber insurance as one component of a comprehensive risk management strategy, however, proactive cyber defenses remain crucial.

Survey guide and methodology

In January 2024, TELUS and its research partner IDC executed a comprehensive survey of Canadian organizations' cyber insurance experiences, challenges, and attitudes.

The 502 survey participants included 84% decision makers and 16% influencers who evaluate and select cyber insurance coverage, with 78% in IT and Operations and 22% from different lines of business. Among final insurance decision makers, 94% also have the final say over their organization's broader cybersecurity strategy and management.

The survey, conducted in English and French, included respondents from organizations of different sizes: small (100-249 employees), medium (250-499 employees), large (599 to 999 employees), and enterprise (1,000 or more employees).

Respondents came from organizations across Canada, with 41% in Ontario, 26% in Quebec, 22% in Western Canada, and 11% in Atlantic Canada. The survey is also representative of a broad range of over 20 commercial and public industry verticals.

By the numbers: cyber insurance in Canada

64%
of Canadian organizations have cyber insurance

16%
had cyber insurance but no longer have coverage

93%
are concerned about maintaining their coverage

68%
of organizations saw a premium increase during their last renewal

2/3
of organizations saw an average premium increase of 19% year over year

1 in 10
organizations are considering insurance but are still undecided

The least likely incidents to be covered by insurance are

- system or business failures
- human error, negligence, or mistakes
- acts of war

To qualify for a policy, 1 in 4 organizations needed to implement or expand security processes or functions and 2 in 5 had to add or improve security controls.

More than a quarter of organizations submitted an insurance claim in the past 12 months

71%
of those receiving payouts say it did not meet their expectations

41%
received a payout that was **smaller** than anticipated while another

29%
received a payout that was **much smaller** than anticipated

Top reasons payouts fall short of expectations

- The policy did not cover all elements of the incident
- The insurers' assessment of recovery costs misaligned with organizations
- The organization found to be non-compliant with policy requirements

Only 18%
feel that they are well protected and prepared for future incidents and claims

34%
say they need a managed security services provider to help manage controls

26%
say they want outside advisory services to better understand their risk

The state of cyber insurance in Canada

A little bit about risk — what it is and what you can do about it

Organizations' attack surfaces continue to grow as they embrace new technologies, introducing new risks that need to be managed and mitigated. Add to this an evolving threat landscape that brings ongoing complexity and you have a challenge that can never be fully addressed. For these reasons, it's important to define and understand your organization's risk tolerance and priorities.

The balance between growth and risk will be different for each organization. For example, those looking to grow fast will likely take on greater risk. Once you've defined your risk tolerance, focus can then turn to managing risk effectively and in a manner that aligns with your risk tolerance.

What is risk?

The possibility of harm or loss to your IT network, systems, and devices, as well as the data stored on these resources and the services they provide across your business operations.

A common risk management technique is the ACAT model:

- **Avoid**: Avoiding risky practices can help eliminate or greatly decrease your exposure to certain types of risk. For instance, prohibiting access to sensitive data from personal devices that are not managed by your organization can help reduce your attack surface.
- **Control**: Implementing technologies such as firewalls and processes like multi-factor authentication (MFA) can help reduce the risks you cannot avoid.
- **Accept**: If you store non-sensitive data in the cloud, a compromise of that cloud data will not necessarily damage your organization. Rather than spending resources to secure non-sensitive data stored in the cloud, you could accept the risk of exposure. If the cost to secure the data is greater than its worth, you're likely to accept the risk.
- **Transfer**: Risk can be transferred to a third-party, such as partners or insurance providers. Transferring the financial burden of various risks to traditional insurance is a long-standing practice.

For Canadian organizations, the reality is that it's no longer a matter of if but when they will experience an incident. This means that maintaining an understanding and strategic approach to managing cyber risk is key. Cyber insurance is an increasingly popular part of many organizations' risk management strategy and recovery tool kit. To better understand why, let's take a look at how prevalent cybersecurity incidents are in Canada.

For Canadian organizations, incidents are common and frequent

To understand how the threat landscape is affecting Canadian organizations and how cyber risk is materializing as incidents, the study examined the prevalence of cybersecurity incidents.

Seventy-six per cent of Canadian organizations experienced an incident in the past 12 months. If an organization has not experienced a cybersecurity attack, they are an outlier. Regardless of business size or vertical, the data shows that organizations are experiencing an average of 3 cybersecurity incidents per year. And while an incident can be anything from a server outage for a few hours to a full-scale data breach, the potential for disruption can be immense.

A **cybersecurity incident** is an event that potentially impacts the confidentiality, availability, or integrity of computer networks, systems, or data.

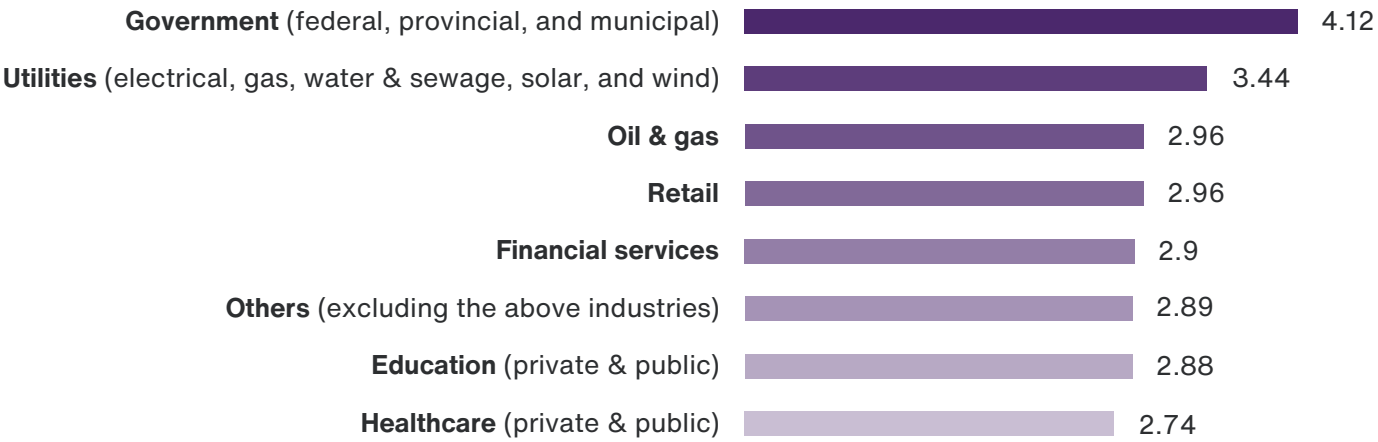
The verticals with the highest rates of cybersecurity incidents per year are:

4.12
Government

3.44
Utilities

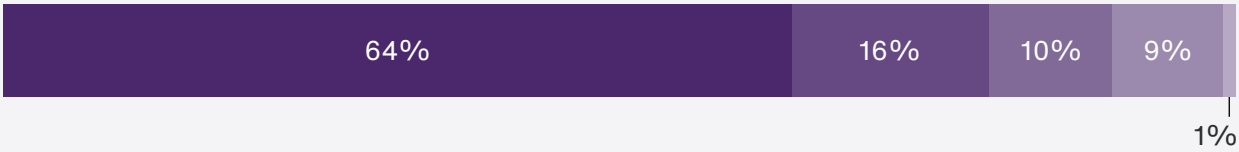
2.96
Retail

Average number of incidents by vertical



So, how do these high incident rates impact Canadian organizations' outlook for the future? Looking ahead, most organizations feel confident about the next 12 months. The majority (78%) believe they are well prepared to respond to a successful cyberattack. Only 28% of organizations perceive that they are at a high risk of a significant financial or brand loss from a cyberattack.

Given the realities of the threat landscape, **most organizations are leaning into cyber insurance**. On average, **64% have cyber insurance currently**, and another 10% are considering it but have not made a decision.



64%

of organizations currently have cyber insurance

- 16% had cyber insurance but are no longer covered
- 10% are considering but have not made a decision yet
- 9% have not considered cyber insurance
- 1% considered and decided not to purchase cyber insurance

Insured organizations by size:

Small
100-249 employees
50%

Medium
250-499 employees
61%

Large
500-999 employees
72%

Enterprise
1000 or more employees
69%

For small organizations, insurance may be a lower priority due to budgetary constraints or a “security through obscurity mindset” — the assumption that they are too small to be a target of cyberattacks. In reality, smaller organizations may be facing greater risk: the data shows that on average, small organizations experienced a higher number of incidents in the past 12 months than enterprise-sized organizations.

Among insured organizations, 86% have a single provider, likely because they don’t need the level of coverage that would entail using multiple providers. By working with a single provider, they’re minimizing the complexities of managing and complying with multiple policies. Only the largest organizations are likely to hold policies with two or more insurers, typically with the purpose of maintaining various coverage brackets. About 1 in 5 (22%) chose to do so or may be required to do so if they want to achieve their payout limits.

Financial fallout from an incident drives the decision to purchase cyber insurance

The motivations for obtaining cyber insurance are unsurprising, given that insurance primarily serves to soften the financial losses of adverse events.

The motivations vary by organization size. While the top driver for larger organizations is financial cost mitigation, midsize organizations want to cover response and recovery costs. On the other side of the spectrum, compliance and regulations are the most important considerations for small organizations.

The priorities driving purchasing decisions also range broadly across verticals. They include:

Covering the **cost of ransom** during a ransomware attack:

Covering the **cost of response and recovery**:

Mitigating **financial loss** due to revenue, downtime & reputation:

Gaining **incident response capabilities** not available in-house:

Mitigating legal and third-party liability due to working with sensitive data:

The majority of Canadian organizations have reservations about cyber insurance

While 64% of Canadian organizations currently have cyber insurance, and some are still considering it (10%), 4 out of 5 admit they have reservations.

Top reservations

- High premiums (17%)
- Lack of incident response flexibility (12%)
- Fear of not being covered in an incident (12%)

Only 1 in 5 organizations expect to be treated fairly by the insurance company and receive prompt compensation.

34% expect somewhat fair treatment and delayed payouts

31% expect insurers to look for loopholes and provide minimal payouts

32% believe they will be treated fairly and will be provided prompt compensation

14% believe they will be denied payouts

Lacking a clear replacement for insurance, organizations often rely on partners to help them better manage risk

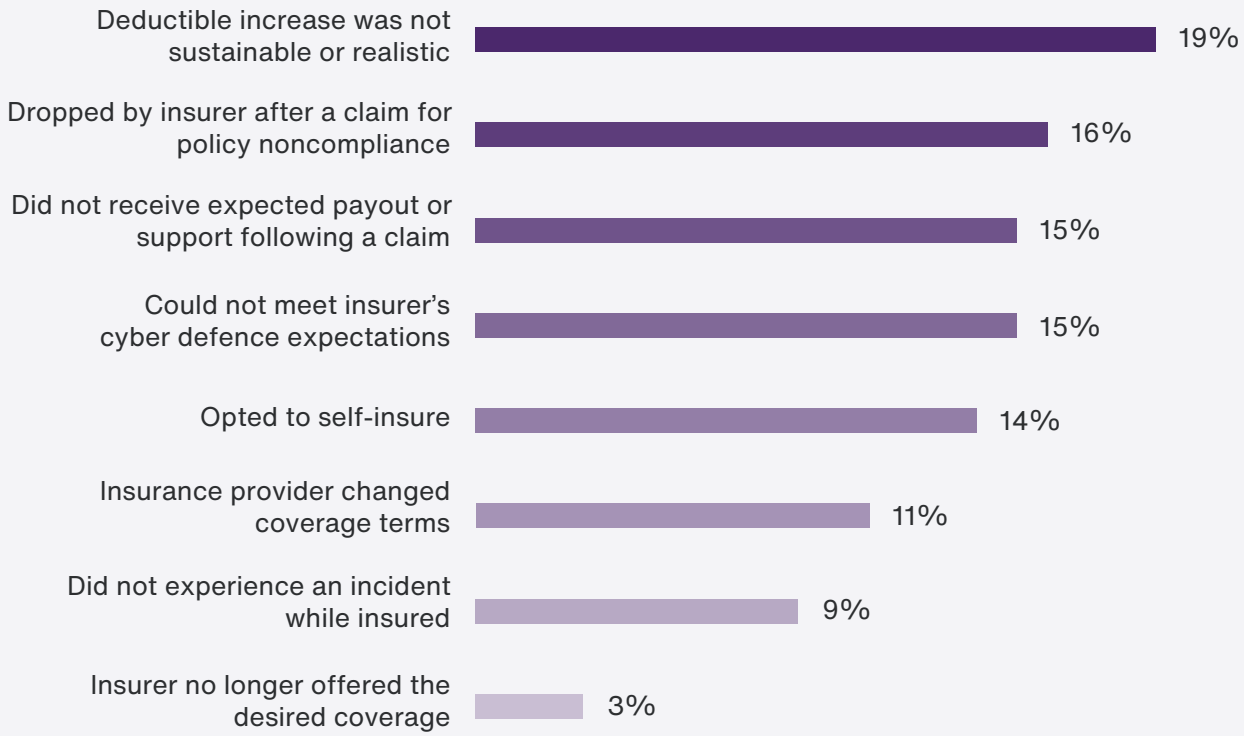
A variety of factors are pushing organizations to manage risk without insurance. These range from high costs of obtaining or maintaining insurance to frustrations over requirements and payout sizes.

Premiums vs. deductibles

A premium is the monthly cost you pay for your insurance policy, while a deductible is the amount of money you must pay before insurance will payout a claim.

Sixteen per cent of organizations discontinued their insurance — and the main reason was an increase in the deductible, making it unsustainable. Some opt out of renewal because the insurance did not meet their expectations (such as a payout amount), or are unable to meet policy requirements. Others are dropped by the insurance company after a claim due to noncompliance.

Main reasons organizations are no longer insured



The reasons for discontinuing insurance vary across organization size. Small and medium-sized organizations are more likely to opt out due to increased deductibles, large ones more likely due to not receiving the expected payout or support, and enterprises due to not experiencing an incident.

Only 1 in 4 organizations with discontinued insurance are seeking a new provider. Instead, most are managing their risk in other ways, without the added safety net of insurance. To do so, these organizations are seeking out third-party experts for both guidance and implementation of their cyber strategies. More than 40% of organizations are turning to outside experts for help improving their security posture, 37% are turning to consulting services for developing alternative cyber strategies, and 26% are reallocating their insurance budget to third-party managed security services.

This data indicates that many organizations lack the expertise and resources they need to understand their security deficiencies and how to address them strategically. Consequently, they are engaging outside experts to help identify gaps in their defences, create a cyber risk mitigation strategy, and allocate funds effectively. By identifying the gaps, security leaders can make a stronger case for the funding that is necessary for security investments. Additionally, many organizations find value in outsourcing their cybersecurity defences to outside partners, whose expertise and resources can help address challenges such as shortage of in-house talent and other resource constraints.

How organizations are managing their risk without cyber insurance

Top 3

Consulting services to improve security posture (42%)

Consulting services to develop an alternate strategy to cyber insurance (37%)

Pursuing contractual risk transfer approach with partners (28%)

Reallocating insurance funds to in-house cyber defence controls (27%)

Seeking a new cyber insurance provider (26%)

Reallocating insurance funds to 3rd party managed cyber defence controls (26%)

Reallocating insurance funds to other business initiatives (22%)

Pursuing a self-insurance strategy (20%)

No other strategies are being pursued (1%)

Cost is the biggest influencer for undecided organizations

One in 10 organizations have either not considered insurance or considered and decided against it. This group is primarily comprised of smaller organizations who cited the following as their top reasons to not adopt cyber insurance at this time:

- **Waiting for the market to mature (38%)**. This point of view likely reflects the experience of different insurance assessment processes and policy requirements. While market maturity may bring standardization to the assessment processes, since insurer requirements are a response to the evolving threat landscape, this aspect of insurance may not stabilize in the same way.
- **Belief that they would not qualify for insurance (36%)**. This may indicate that those organizations think they would need to mature their processes and/or controls to meet insurer standards.
- **Belief that there are better alternatives to cyber insurance (36%)**. These organizations may feel their money would be better spent on additional controls or outsourcing their defence, rather than on premiums.

So, what would convince Canadian organizations that are considering insurance to move forward with a policy? First and foremost, cost. **Half of organizations that are on the fence about insurance named cost as the biggest influencer.**

The second most influential factor is if an organization suffers a catastrophic cyber incident. More than a third of organizations across all sizes identified this driver. This rationale may be attributable to the challenge of justifying the expense of insurance to leadership without the experience of an incident.

Third, organizations cited that if insurers were more **flexible with the controls required to maintain a policy** they may consider purchasing insurance.

Top 5 factors that would prompt an organization to consider purchasing cyber insurance in the future

- Lower cost options
- A catastrophic cybersecurity incident
- Greater flexibility with required controls
- Cyber insurance market maturity
- Starting to work with or store sensitive data

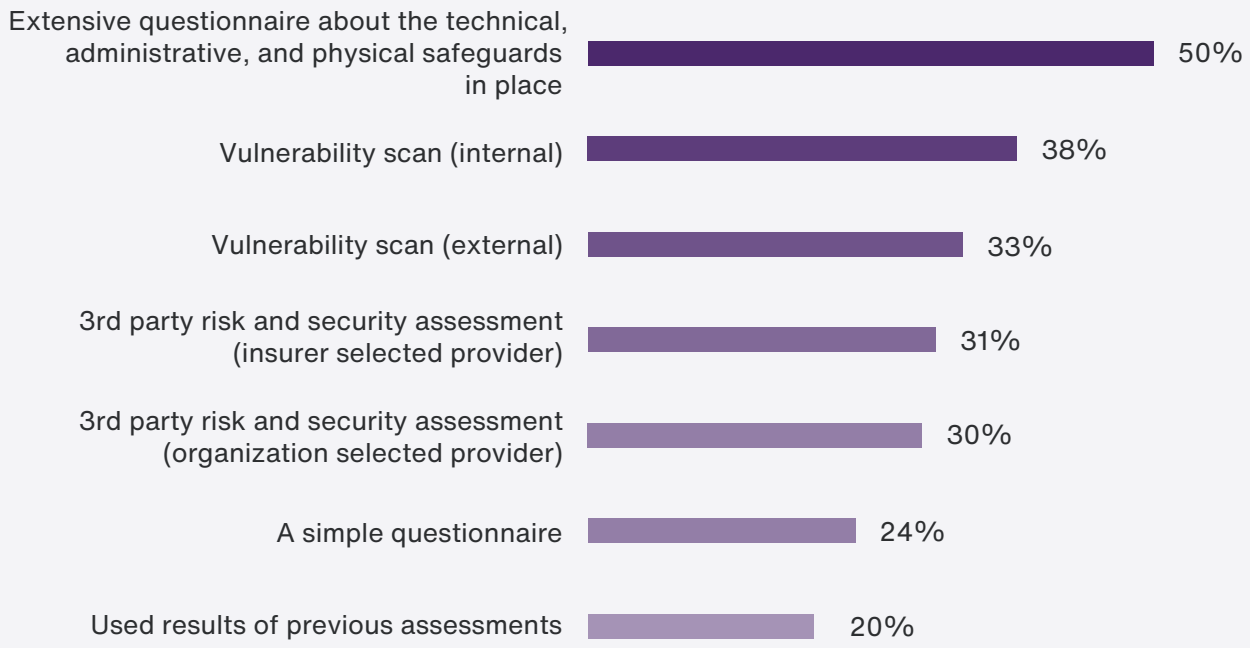
The realities of obtaining and maintaining cyber insurance

Canadian organizations are shopping around, engaging with an average of three insurance providers before selecting policies. The majority (85%) are working directly with an insurance company rather than a broker.

An **insurance broker**, who serves as an intermediary between the organization and the insurance provider, can help simplify and reduce the burden of the application process.

For each insurance provider, an organization may be asked to complete an extensive questionnaire, engage with third-parties to validate their cybersecurity posture, provide proof of compliance with regulatory requirements, or a combination of these depending on the desired coverage. A broker works with the customer to collect this information and then can tailor it to the requirements of different insurance providers.

Assessment methods used by insurers



Although the application process remains a heavy lift for organizations, 97% indicated that they had a positive experience during the application process, due to the following:

Improved security posture helps avoid higher premiums and deductibles

Insurers may require improvements to processes and controls based on their assessment of an organization's security posture, risk exposure, their experience with past claims and the current threat landscape. The following graphic shares the top processes and controls that organizations initiated, adopted, or advanced to meet insurance requirements and/or lower the cost of coverage:

Top processes & controls

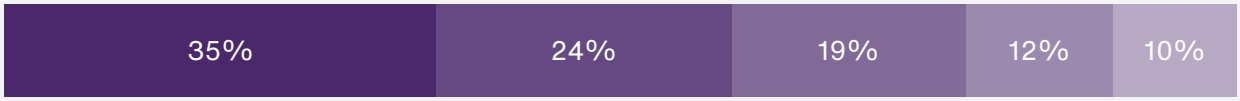
1 in 4 organizations had to improve processes or functions

1. Security Operations Center (SOC)
2. Security awareness program
3. Vulnerability management program
4. Patch management
5. Disaster recovery

2 in 5 organizations had to add or improve controls

1. Identify and Access Management (IAM)
2. Security Information and Event Management (SIEM)/ log management
3. Data security
4. Privileged Access Management (PAM)
5. Managed Detection and Response (MDR)/Extended Detection and Response (XDR)

Impact to organizations opting to not make the requested additional investments



- 35% Higher premiums
- 24% Loss of coverage
- 19% Higher deductibles
- 12% Policy not issued or cancelled
- 10% No impact, investments were optional

1 in 5

organizations switched their cybersecurity vendors based on input from their insurance provider

Although complying with insurance companies' requirements may be challenging for some organizations, the mandated improvements and enhancements serve to improve their cybersecurity posture. Insurance requirements can also help security leaders obtain funding for improvements proactively rather than after a costly incident.

It can be a heavy lift for organizations to formalize processes and roll out new controls. Many seek the help of security service providers as a result to help them maintain policy compliance. This may include consulting to better manage their risk exposure and managed services to aid with functions that require 24x7x365 support, like threat monitoring and response.

Organizations renewing policies are likely to see rising premiums

Rising premiums are a trend across the cyber insurance industry and may be attributable to a few factors, including more insured organizations filing claims, the evolving nature of the threat landscape, and insurers exploring new ways to balance costs while providing effective coverage. Among currently insured organizations, over two-thirds **saw an average increase of 19% in their premium** during their last renewal. Unfortunately, some organizations are facing renewals with higher premiums and lower coverage.

19%

the average premium increase organizations saw when renewing their cyber insurance policy

Cost and coverage, here's what to expect

An organization's cyber insurance premiums and deductibles are influenced by a number of different factors, some of which are in their control and others that are not. These can include:

No control

- The vertical or industry of the organization
- The type of data the organization has
- Thirty-party partners security posture
- Trends within the cybersecurity landscape

Can control

- Past claim history
- Cybersecurity posture (people, processes and tools)
- Selecting third-party partners
- Compliance to industry standards and government legislation

Average premiums, deductibles and payout limits by organization size

	Average across all sizes	100-249 employees	250-499 employees	500-999 employees	1000 or more employees
Premium	$148K	$18K	$31K	$60K	$537K
Deductible	$1M	$154K	$303K	$441K	$3.6M
Payout limit	$94M	$14M	$19M	$43M	$345M

When examining the relationships between premiums and deductibles, as well as premiums and payout limits, the data indicates that premiums constitute 14.3% of the deductible amount and 1.1% of the payout limit. These ratios may be a useful benchmark for comparison and provide you with a baseline for your organization.

	Average across all sizes	100-249 employees	250-499 employees	500-999 employees	1000 or more employees
Premium/ deductible	14.3%	11.7%	10.4%	13.7%	14.9%
Deductible/ payout	1.1%	1.1%	1.6%	1.0%	1.0%

As is standard with insurance policies, cost is often associated with the level of coverage the organization requires. That being said, having an adequate payout limit is only half of the story. Organizations should ensure that they have the breadth of coverage required for the incident types, recovery and response costs they're likely to face. Unfortunately the data suggests that this may not be the case.

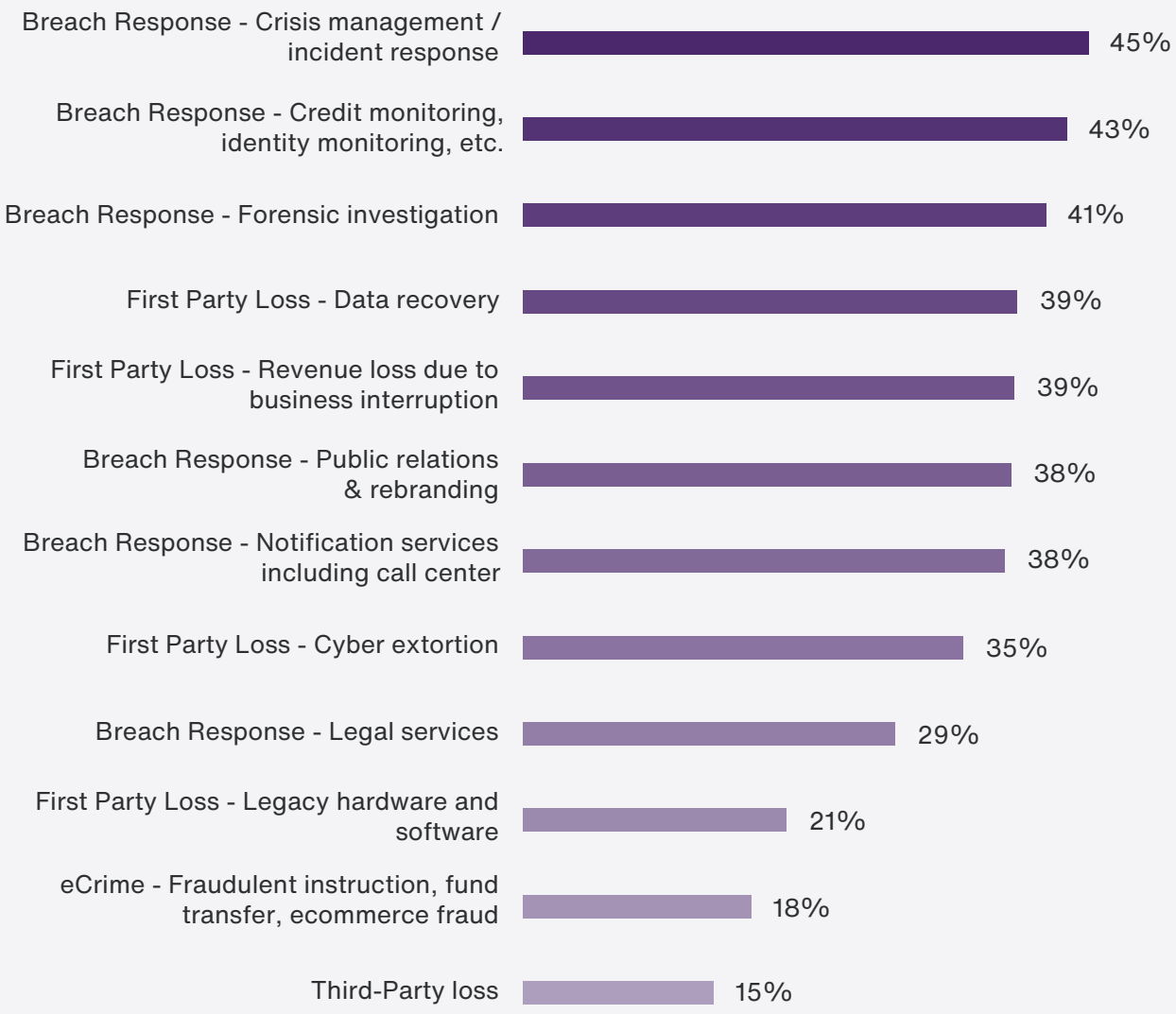
Top 3 **types of cyber incidents** least likely to be covered by cyber insurance policies

- System or business failures
- Human error, negligence
- Acts of war

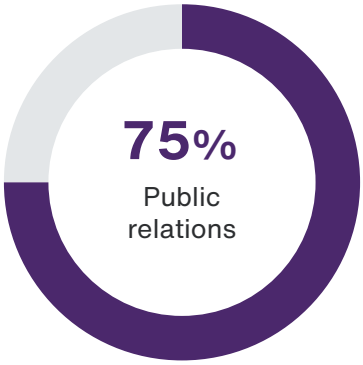
Top 3 **recovery costs / losses** least likely to be covered by cyber insurance policies

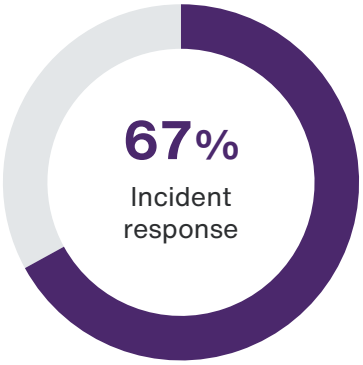
- Third party loss
- Fund transfer, ecommerce fraud
- Legacy hardware and software

Items commonly included in cyber insurance policies



Many cyber insurance policies dictate which third party vendors and service providers that an organization can leverage during a cybersecurity incident to aid in the response and remediation items above. If choices are available, it's important for an organization to have its preferred vendors selected and potentially on retainer to reduce response times when an incident occurs. The following highlights which services organizations **could not** select with their preferred providers during the claims process:





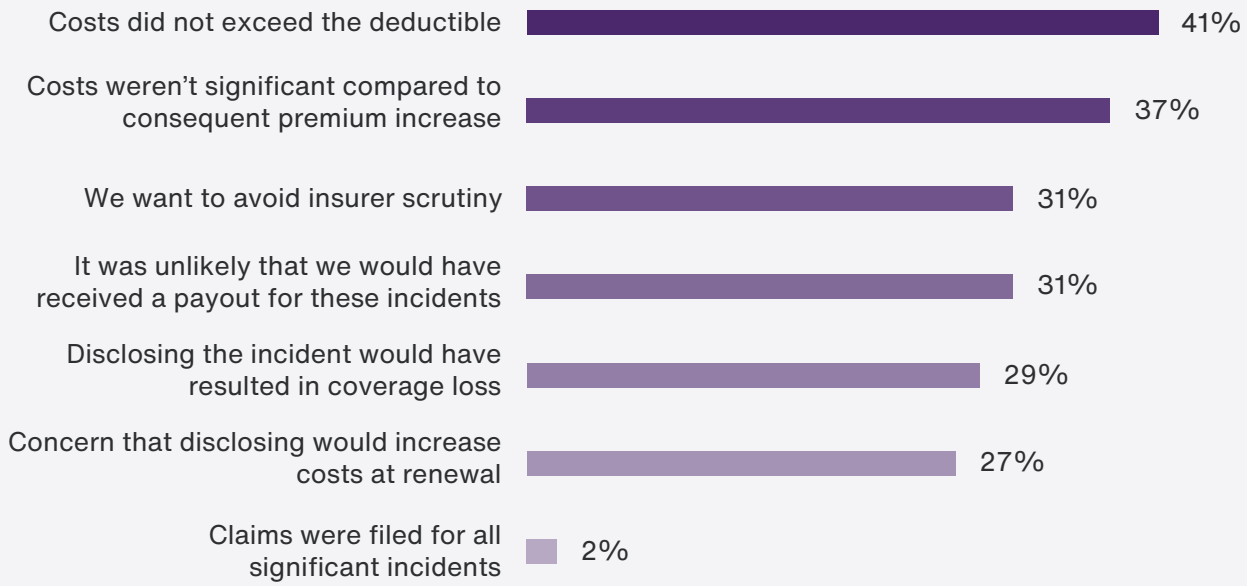
All told, Canadian organizations' experience with cyber insurance to date underscores the importance of understanding your coverage, including the definitions of various categories and the policy limitations and exclusions. Whether you are working with a broker or directly with a provider, identify your organization's needs before purchasing insurance and understand how your policy addresses those needs. These steps will help you avoid surprises during a claim and plan for contingencies for the areas not covered.

Claims process: experience and outcomes

Even when Canadian organizations invest in getting and keeping cyber insurance, they seem to be very careful about deciding when to file a claim. Many are hesitant to file claims, even when it comes to severe incidents.

Of insured organizations, 29% reported submitting a claim. **Only 2% of these organizations indicated that they filed cyber insurance claims for all the significant incidents they experienced.**

Reasons organizations opted against submitting a claim



Payouts are common but often smaller than anticipated

Seventy-seven per cent of organizations that submitted a claim in the past 12 months received an insurance payout. While this demonstrates how reliably insurers pay out for claims, it's important to consider the experience of two groups:

77%
received payouts from submitted claims

23%
did not receive pay out

29%
payout met expectations

41%
payout was **smaller than expected**

29%
payout was **much smaller than expected**

Top 3 reasons insurers provided payouts that were **smaller** than expected

1. The **policy did not cover all elements of the incident** they experienced, like ransom payment.
2. The **insurer's assessment of recovery costs was misaligned with those of the organization.** This may include costs of recovery tools or additional third-party support required beyond initial incident response activities covered by the insurer.
3. During the claims process, the **insurer discovered the organization did not fully comply with policy requirements.** For example, this could include controls not being extended to new environments during the course of the policy.

When an incident occurs, one of the insurer's first orders of business is to ensure compliance with the policy. This demonstrates that organizations need to focus on understanding and fully following policy requirements from the time the policy is issued, throughout its term, and during renewal. It may be challenging, as an organization's technology environment and stakeholders will evolve over time.

For the 23% that did not receive a payout, reasons include:

- Payouts for the term reached coverage limits
- The root cause of the incident was not covered by the policy
- The insurer discovered the organization did not fully comply with policy requirements
- The security incident was not in the scope of coverage
- Claim was denied based on a technicality

On average, cyber insurance claims only cover 60% of the cost of an incident

Comparing incident costs to claim payouts, it's not hard to see why organizations' payout expectations are frequently unmet.

	Average incident cost	Average claim payout
100-249 employees	$2.1M	$1.1M
250-499 employees	$2.0M	$1.1M
500-999 employees	$4.3M	$2.5M
1000 or more employees	$21.3M	$13.3M
Average across all sizes	$6.5M	$3.9M

Recovery costs are often significantly higher than anticipated

Ninety-six per cent of organizations underestimated the costs associated with a major incident. Why is this? A lack of experience managing significant incidents may result in organizations not obtaining high enough payout limits, and/or not obtaining the sufficient breadth of coverage to include all applicable costs.

The top three incident costs that were significantly higher than anticipated were crisis management and incident response (53%), losses due to business interruption (49%), and cyber extortion costs such as data recovery and ransom (34%).

Incident costs that were significantly higher than anticipated

53%
Crisis management/ incident response

49%
Business interruption

34%
Extortion payment - ransom, data recovery

33%
3rd party - identity & credit monitoring, regulatory fines

28%
Others - fraudulent transactions, eCrime, etc.

26%
Legal fees

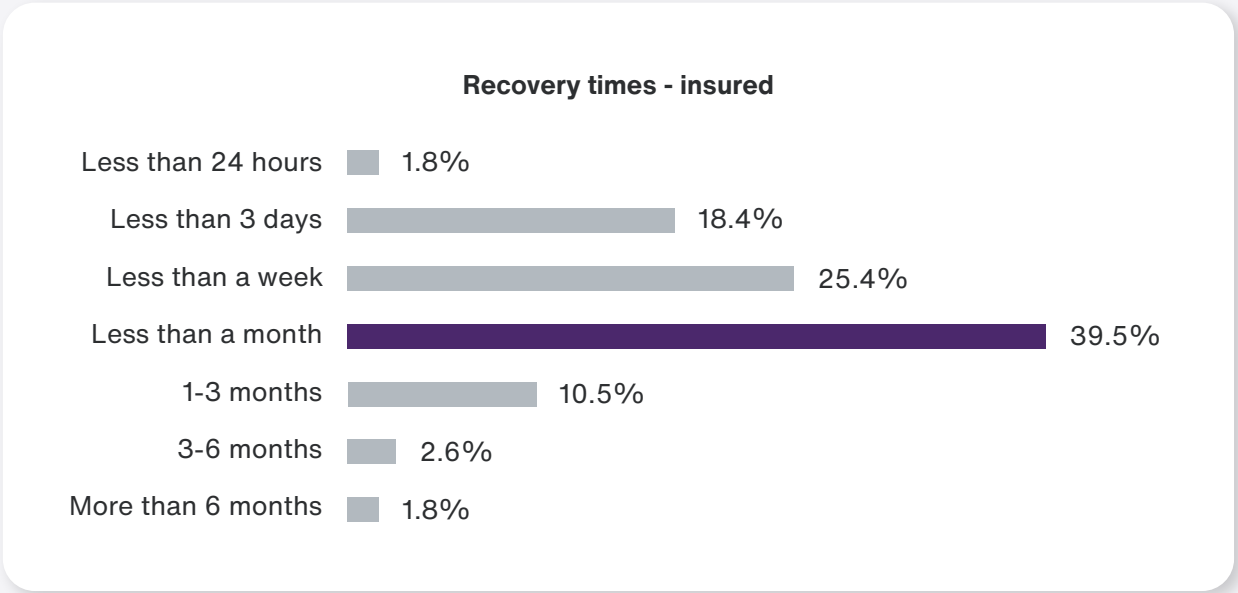
25%
Public relations

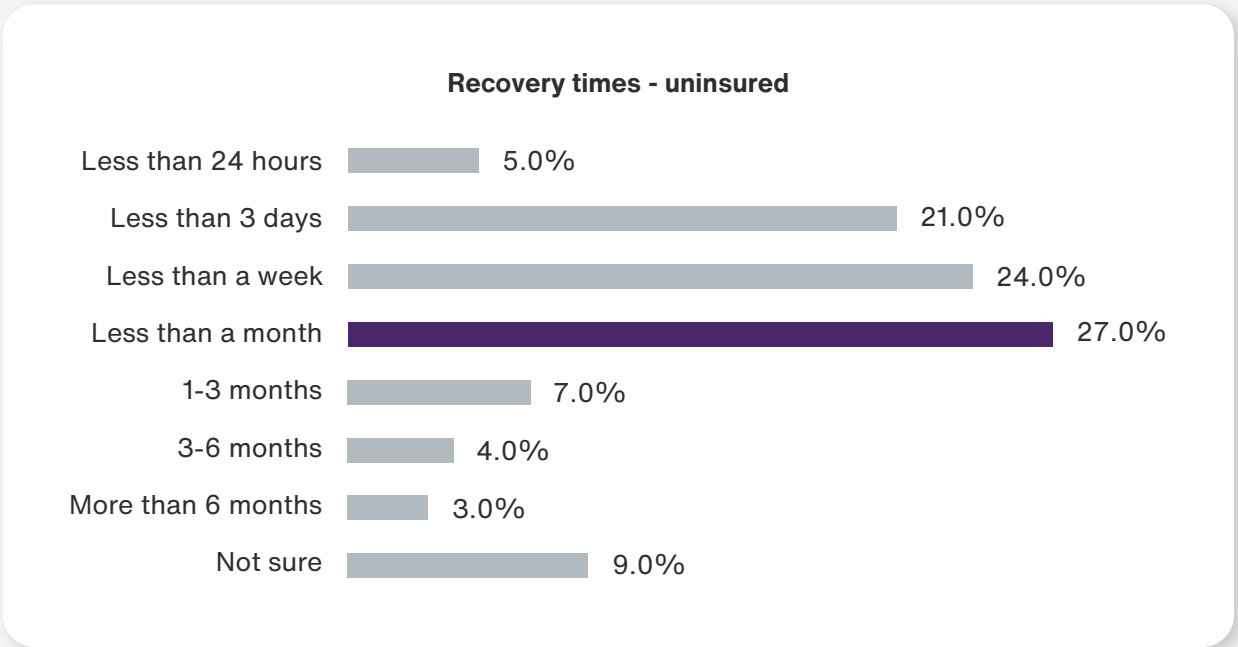
8%
Notification services

96%
Indicated that incident costs were higher than expected

For over three quarters of organizations (76%), an additional source of unexpected costs was having to engage additional third-party support beyond what was supplied by their insurance provider. Specifically, 30% of organizations engaged incident response services and 28% engaged digital forensics services while 18% had to engage additional third-party support for both. This may be because the required support fell outside of the policy coverage or exceeded payout limits.

When it comes to response and recovery times, the claims process does not appear to slow these processes down. The average recovery time, for both insured and uninsured organizations, is less than a month.





Organizations that have experienced the claims process come away with lessons learned

Eighty-two per cent of organizations shared they feel unprepared for their next significant cyber insurance incident and/or claim. In order to improve their ability to identify and respond to threats quickly, organizations have identified a number of top priorities, including:

- Gaining better visibility across their attack surface (28%)
- Improving incident response plans (28%)
- Improving detection and response measures (25%)

To improve future outcomes, 26% of organizations are taking a thoughtful approach to understanding risk by seeking help from third party advisory services. Additionally, 21% have identified that their executives need a better understanding of risk. With 11% believing that they don't have enough coverage for cyber incidents, engaging the C-suite and board of directors in conversations about cyber risk can be an effective way to educate this layer of the organization and prioritize cyber insurance spend.

Recognizing the need to better maintain compliance over the course of their policies, 34% of organizations are turning to MSSPs to address control gaps and resource shortages. An outside security provider can bring valuable knowledge and resources that help organizations ensure they comply with requirements.

Every organization is unique and will have its own risk tolerance and preferred risk reduction strategy. How cyber insurance plays into that will be similarly unique. It's important to view this process as a journey, not a "one-and-done" activity. As the threat landscape evolves and organizations continue to transform, they must constantly reassess their insurance needs and cyber priorities.

Getting the most value from cyber insurance for your organization

When asked to think about their future, the majority of Canadian organizations (93%) expressed concerns about maintaining their coverage including:

- Unaffordable premiums (32%)
- Lack of funding to maintain compliance with the policy requirements (30%)
- Inability to complete the application questionnaire (17%)
- Change of direction or lack of support from management or the board of directors (14%)

With concerns running the gamut from costs to process and strategy, it can be difficult for organizations to drive the best value from cyber insurance. Insights from this study suggest the following considerations are key to improving your security posture and should put your organization in a good position to obtain sufficient cyber insurance coverage.

Proactively prepare your organization for assessment

Assess and define your risk tolerance and coverage needs.

What are your organizational goals and how fast are you looking to achieve them? How much coverage is enough? Do you have to comply with any contractual obligations for coverage limits? To answer these questions, it's important to leverage the data at your disposal including the cost of recovery for past incidents and the payout for past claims if applicable.

Having a clear understanding of your risk tolerance and coverage needs will best position you to assess the policies offered to you by insurance providers following the application or renewal process.

Understand your posture and gaps.

Before engaging with a broker or insurance provider, conduct risk assessments, vulnerability scanning, and/or a regulatory or security standard compliance audit to identify existing gaps, along with the improvements an insurer is likely to request. And, if possible, address these gaps before engaging in the application process.

Understanding and being able to demonstrate adherence to known and trusted frameworks like NIST, ISO/IEC 27001 or others, can make your application process smoother.

Deploy the processes and controls insurers most often require

Proactively addressing security gaps in your environment before applying for or renewing insurance can enhance your security posture, satisfy common insurer requirements, and help you avoid higher premiums, deductibles, or reduced coverage.

Review your processes and evolve them as needed.

The processes and functions that organizations in this study had to most often improve to meet cyber insurer requirements are not new and are likely already part of your strategy in some way. These common areas include security awareness programs, vulnerability management programs, patch management, and disaster recovery.

Take some time to assess and determine if these processes and functions could be improved, either by adding a solution like a patch management tool or engaging a third-party consulting partner to help formalize these processes.

Ensure your controls are effective and extend to all areas of your environment.

Forty per cent of organizations had to add or improve their controls around Identity and Access Management (IAM), Security Information and Event Management (SIEM) and/or log management, data security, Privileged Access Management (PAM), and Managed Detection and Response (MDR)/Extended Detection and Response (XDR). Assess the current controls in place to ensure they extend into all areas of your environment (cloud included) and are managed and resourced appropriately.

To limit damage and optimize recovery time, wisely invest in your response and recovery tool box

The data makes it clear that organizations are underestimating the cost and complexity of recovery.

- 96% indicated that incident costs were higher than expected
- 76% had to engage with additional third-party services beyond those supplied by their insurer for incident response and digital forensic services
- 53% cited crisis management/incident response as the number one cost that was significantly higher than anticipated

This highlights the importance of proactively managing your risk and security posture, including investing in your organization's response and recovery toolbox. What does this look like in action? Consider having an incident response retainer in place, as well as a formalized, current, and tested incident response plan. You may also want to consider immutable back ups, which cannot be altered in any way, that grant you the ability to recover to a trusted state.

Consider using an insurance broker.

While 85% of Canadian organizations worked directly with an insurance provider versus a broker, they still engaged on average three different insurance providers during the application process. Depending on your coverage needs and desire to shop around, a broker may help reduce the lift for your organization when it comes to completing questionnaires and negotiating a policy.

Don’t set it and forget it - maintain policy compliance as your environment evolves.

An organization's IT environment will likely change over the course of their policy term. Be sure to keep this in mind and apply policy requirements to those changes as they occur. This will help you avoid any surprises during renewal time or denied claims should your organization experience an incident.

Every organization’s journey will be unique

You may not need to invest in all of the above processes and controls; in fact, the prospect of doing so may be overwhelming or unrealistic. Instead, use these suggested strategies as sound security options that can help improve your posture and best prepare you to obtain and maintain insurance coverage.

If you are short on resources or aren’t sure how to apply these strategies to your unique needs, working with a cybersecurity partner can provide clarity. Engaging an expert partner will also alleviate pressure from your IT and security teams, allowing them to focus on other priorities while ensuring your organization gets the comprehensive protection it needs.

About TELUS Business

TELUS empowers businesses to thrive in a digital world. Having partnered with Canadian organizations to support their evolving cybersecurity needs for over 20 years, TELUS understands the security threats and challenges businesses face every day.

Our intel, expertise, and comprehensive suite of managed and professional services are designed to meet the advanced security needs of your business. Gain peace of mind knowing you've partnered with a cybersecurity leader you can rely on.

To learn more how to better protect your organization, visit telus.com/Cybersecurity

Read more TELUS landmark Canadian studies

Get your copy of our previous studies today:

The TELUS Canadian Cloud Security Study

telus.com/CloudSecurityStudy

The TELUS Canadian Ransomware Study

telus.com/RansomwareStudy

Appendix

This report presents a general study of the cybersecurity insurance market for businesses of various sizes. The information contained herein is based on data available at the time of the study and is intended for informational purposes only. It is important to note that the results and findings presented in this report may not directly reflect or apply to your specific business, industry, or unique circumstances. The cybersecurity insurance landscape is complex and dynamic, with numerous factors influencing policy coverage, premiums, and outcomes.

Readers should be aware that many variables can impact cybersecurity insurance policies and their effectiveness. These factors include, but are not limited to, company size, industry sector, geographic location, existing cybersecurity measures, regulatory environment, claims history, risk profile, and specific policy terms and conditions. Additionally, the rapidly evolving nature of cyber threats and technological advancements may affect the relevance and applicability of certain findings over time.

While this report aims to provide valuable insights into the general landscape of its subject matter, it should be used as a starting point for your decision-making process rather than a definitive guide. This study does not constitute professional advice, legal opinion, or a recommendation for any particular course of action. The authors and publishers of this report make no representations or warranties regarding the accuracy, completeness, or suitability of the information provided for any specific purpose. Readers are strongly encouraged to conduct their own due diligence and seek professional guidance before making any decisions based on the contents of this report.