The TELUS Canadian Ransomware Study

TELUS Business

Table of Contents

TELUS Business

From the desk of Carey Frey, TELUS Chief Security Officer

On behalf of the TELUS Cybersecurity team, I'm excited to share the TELUS Canadian Ransomware Study with you. Given the dramatic increase in ransomware seen across the globe, we wanted to take a closer look at how this growing threat was impacting businesses here in Canada and share insights on how organizations can most effectively protect their business, data and fellow Canadians.

Reflecting back on 2021, it proved to be another arduous year for Canadian organizations across multiple fronts. Nothing can compare to the toll the COVID-19 pandemic had on our families, friends, and businesses, but unfortunately we also had to endure a record year for ransomware incidents and infections affecting millions of Canadians nationally.

In response to the COVID-19 pandemic, Canadian organizations showed amazing agility and resilience in the face of adversity as they shifted how, and where they work and interact. Unfortunately for some, this agility came at the price of thorough cybersecurity risk management. The quick adoption of the new technologies also introduced new vulnerabilities and misconfigurations that could be leveraged by threat actors to deliver ransomware packages. Meanwhile, as organizations worked to evolve during the pandemic, so too have the tactics and malware that threat actors are leveraging. The reality is that with the introduction of tools like ransomware-as-a-service, the barrier to entry has lowered, making ransomware a profitable and easy option for threat actors.

For this in-depth Canadian ransomware study our goal is to educate Canadian organizations on the threat ransomware poses to them and what differentiates organizations that successfully mitigate ransomware attacks. While our findings may paint a grim picture of the current state of ransomware in Canada, there is hope. In the following pages there's much to be learned about the value of a proactive layered defence and how proper processes, technologies, and training help reduce the impact of incidents and the costs associated with them. We've also included a section on best practices, where the TELUS Cyber Defence Centre team shares their thoughts on how Canadian organizations can improve their cybersecurity postures today.

I hope you find this study meaningful and the insights we've shared help inform your cybersecurity strategy and investments. If nothing else, this study shows how the old adage - *an ounce of prevention is worth a pound of cure* - rings true. While no single measure can make your organization impenetrable, proactive preparedness ensures you're ready and able to manage and limit the impact of the threats of today and tomorrow.

Thank you and stay safe,

Carey Frey - Chief Security Officer & Vice President, TELUS Security

Survey guide and methodology

In the summer of 2021, TELUS and its research partner IDC designed and executed a comprehensive survey of ransomware experiences and attitudes among Canadian organizations. The objective was to understand how businesses and the public sector are responding to the threat of ransomware:

- attitudinally
- behaviourally
- experientially
- in their expectations for a response

The survey included 463 respondents from organizations with 50 or more employees, drawing on the experiences of IT leaders and decision makers who had influence or primary decision-making responsibility regarding their organization's cybersecurity. Ninety-five percent of respondents were decision makers, and 5% were influencers; 80% of respondents were "very knowledgeable" about their organization's cybersecurity strategy, and the remaining 20% were "knowledgeable."

The survey, conducted in the respondent's choice of English or French, spanned all regions of Canada and balanced respondents across four sizes of business, ranging from 50–149 employees to 1,000 or more. The study encompassed all industry verticals, with particular focus (quota) on eight sectors: Financial Services, Municipal government, Education, Health, Agriculture, Oil and Gas, Retail, and Utilities.

By the numbers: Ransomware in Canada

83% reported attempted ransomware attacks

67% experienced a ransomware incident

44% paid the ransom

42% had data fully restored

Verticals that experience the most ransomware incidents

- Healthcare
- Agriculture
- Financial

$140K
average ransom paid
Represents 16% of total cost of recovery

Additional costs of ransomware

- Delayed or cancelled IT projects
- Loss of employee productivity
- Delayed or cancelled business investments

Top 3 attack vectors in Canada

1. Misconfigurations
2. Email/Phishing
3. Known vulnerabilities

63% of victims experienced a multiple extortion attack

62% of organizations lack active, 24x7 monitoring

24% took weeks to months to contain and eradicate their last ransomware incident

Top remediation challenges

- Containing the incident
- Quick & coordinated response
- Root cause analysis

TELUS Business

Ransomware: Threat to the digital economy

Organizations are operating in a new reality; the pervasive increase in ransomware seen over the last 24 months has left many organizations struggling to stay ahead of the threat. Around the world, ransomware attacks are bringing organizations, and the communities they serve, to a grinding halt. No one is immune. Every entity — from critical national infrastructure providers, local and federal governments, and large enterprises to schools, hospitals, and local businesses — are all vulnerable to the pandemic of ransomware.

What is ransomware?

Ransomware is a type of malware that blocks access to or encrypts the files on target IT systems, rendering any files and the systems that rely on them unusable. Malicious actors then threaten to destroy or publicly release your data unless you pay a ransom in exchange for decryption.[1]

Common attack vectors

Phishing

A phishing email is received, containing a malicious link or attachment.

Malware is introduced to the device and potentially the broader network upon clicking on the malicious content.

Threat actors are able to access, steal and/or encrypt information.

Malicious websites

User mistakenly visits a malicious website and downloads malware.

With this download, malware is introduced to the device and potentially the broader network.

Threat actors are able to access, steal and/or encrypt information.

Compromised credentials

Using stolen credentials, threat actors access the company network and deploy malicious code.

With access to the network (barring the use of additional security measures like MFA), threat actors are able to access, steal and / or encrypt information.

Known vulnerabilities

Threat actors exploit known vulnerabilities to attack and access environments that have not been adequately patched.

Upon gaining access, threat actors are able to access, steal and / or encrypt information.

TELUS Business

[1] https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099

How big is the problem?
(hint: it's big)

To boost collaboration, streamline operations, and improve customer experience, Canadian businesses have embraced digital technologies like cloud, operational technology (OT), Internet of Things (IoT), and data analytics. The shift to remote work, which rapidly intensified during the COVID-19 pandemic, has fundamentally changed business processes. Organizations from coast to coast have quickly adopted new and unfamiliar digital workflows as part of their digital transformation initiatives.

The problem? For many Canadian organizations, quick adoption occurred without proper assessment of the complexity and cybersecurity risk of these new technologies. Many organizations were forced to adopt a mindset of "adopt first and secure later," which has resulted in new vulnerabilities and elevated cyber-risk.

Not only have businesses shifted how they operate - customers have embraced ecommerce with online purchases surging by 99% during the pandemic.[2] All of these changes have brought with them new cybersecurity risks for organizations and new opportunities for threat actors to exploit.

As our survey respondents have reported, cybersecurity is one of the greatest risks to business operations today.

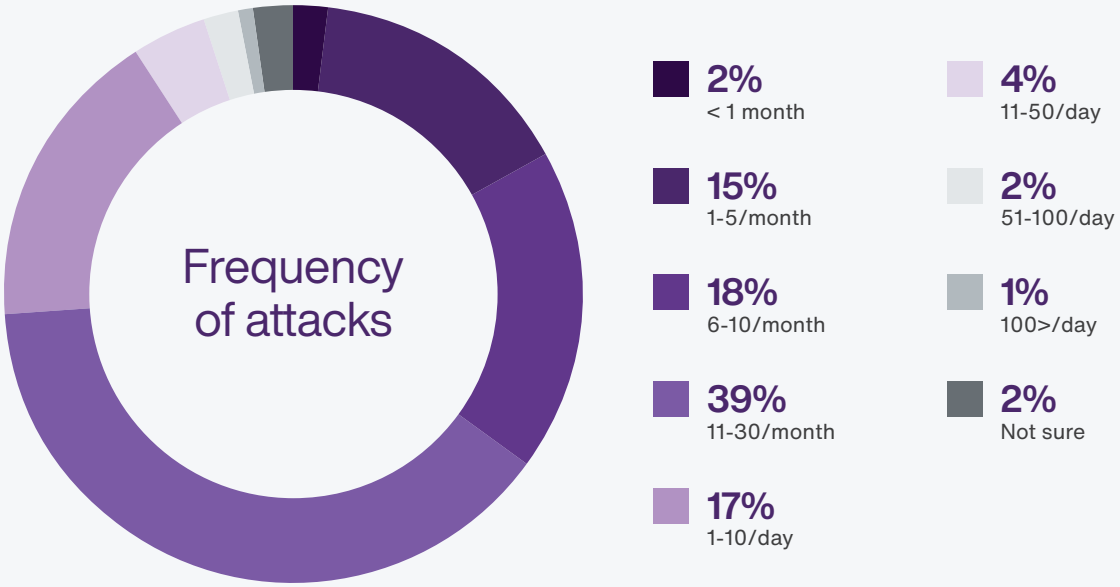
TELUS Business

[2] https://www150.statcan.gc.ca/n1/pub/45-28-0001/2020001/article/00064-eng.htm

Cybersecurity attacks are growing in frequency and severity

Cyberattacks are on the rise in Canada, with 98% of Canadian organizations reporting a cyberattack in the last 12 months. Attacks are **frequent**, with 25% of organizations experiencing at least one attack per day and most organizations experiencing more than 11–30 attacks per month.

More than one-third of organizations experience cybersecurity attacks between 11 and 30 times a month.



Q: On average, how often does your organization experience cybersecurity attacks? (phishing, ransomware, social engineering, etc.)

Ransomware: Behind the growing numbers

Ransomware is emerging as the most serious concern for security teams in Canada. **Across industry verticals and organization size, 83% of Canadian organizations reported attempted ransomware attacks.**

Why is ransomware so rampant? There are a few reasons. First, as adoption of digital transformation technology increases, an organization's IT complexity, blind spots, and attack surfaces grow, and the probability of a ransomware attack goes up.

Second, ransomware is a very profitable and low-risk crime that is easy to execute. The introduction of the ransomware-as-a-service model makes exploit kits widely available and more affordable. With victim negotiation and payment management simplified, threat actors no longer need to be technically savvy or make large financial investments.

Meanwhile, with many businesses willing to pay a ransom to resume operations quickly (in nearly impossible-to-trace digital currencies) and demonstrating hesitancy to report the incident, leveraging ransomware has made cybercrime more lucrative than ever.

83% reported attempted ransomware attacks	67% experienced a ransomware incident

Large or small, your organization is vulnerable

Overall, **67% of respondents reported experiencing a ransomware incident**. Although 67% may seem quite high, it's important to keep in mind that a ransomware incident can be as simple as a payload being delivered onto an endpoint through a malicious email and may not necessarily have a detrimental effect on the organization or its assets. While some of the incidents included in this statistic have been quite serious, the majority likely weren't. On average, Canadian organizations experienced 3.1 ransomware incidents in a 12-month period.

Larger organizations (more than 1,000 employees) average more attacks than the mean: 3.7 versus 3.1. This is not surprising, given that attacks increase as an attack surface grows wider. Large organizations by their very nature deploy more endpoints and cloud assets to support daily operations, increasing their exposure.

Organizations experience an average of 3.1 successful attacks each year

Percentage of organizations experiencing ransomware incidents

The verticals experiencing the highest average number of ransomware incidents are

Healthcare **Agriculture** **Financial Services**

Smaller organizations are far from immune. The average number of ransomware incidents for small organizations is perilously close to the national average at 2.9 (versus 3.1). As the data shows, no organization is too small to be attacked, and believing otherwise can be costly. Clearly, it's not about "if" but "when" — and now is the time to prepare.

TELUS Business

Is it ransomware?

Delays in classification may lead to delays in recovery and remediation

Classifying a cyberattack as ransomware is challenging for 32% of survey respondents. Why? For one thing, adversaries are continuously evolving techniques, tactics and procedures (TTPs). In addition, they cause confusion and put pressure on security teams by launching attacks on multiple fronts. For example, they may launch an attention-grabbing DDoS attack on the web application infrastructure along with a quieter, harder-to-notice parallel ransomware attack.

Organizations can often make the distinction between locker ransomware and crypto ransomware, but further classifying the type of ransomware (Locky, WannaCry, Ryuk, etc.) is crucial to identifying the dangers posed by the attack and triggering the appropriate response actions.

Whether the delay in detection and classification arises from the attacks being a new threat, the lack of appropriate tools for triaging and investigation, lack of access to comprehensive threat intelligence, lack of resources and expertise, or the inability to quickly classify the ransomware attack, the delay provides adversaries with much-needed dwell time for lateral movement and encryption. Once the attack is successful, this initial delay has cascading impacts on recovery and remediation timelines.

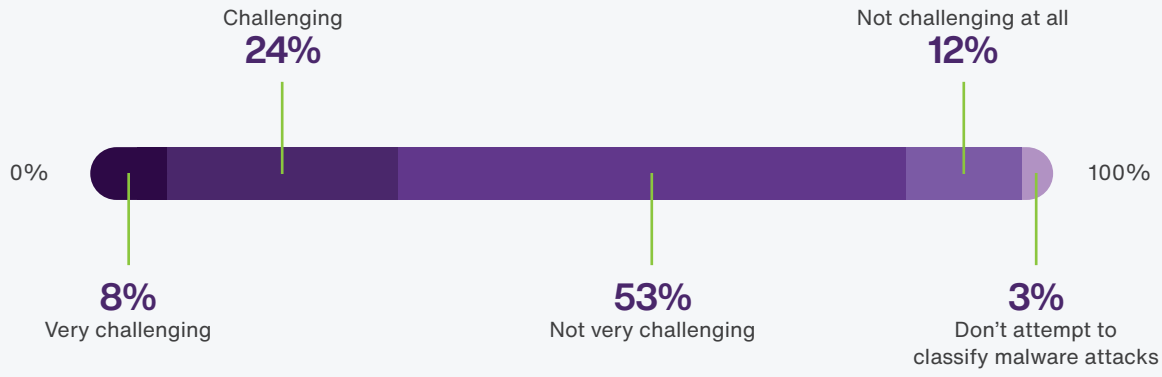
What is locker ransomware?

Locker ransomware is a type of malware that blocks access to basic computer functions or IT systems until a sum of money is paid.

What is crypto ransomware?

Crypto ransomware is a type of malware that encrypts the victim's files, leaving them visible but inaccessible until a sum of money is paid.

Classifying a cyberattack as ransomware is challenging for 32% of respondents.



Q: How challenging is it for your organization to classify suspect attempted cybersecurity attacks as Ransomware Attacks?

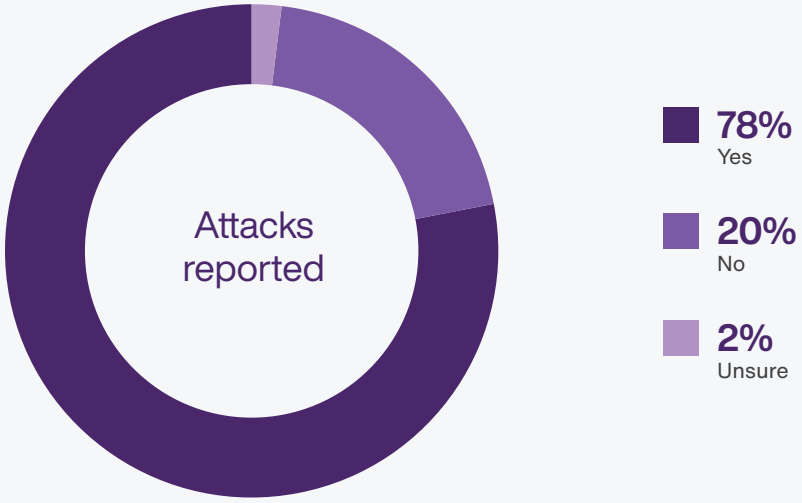
TELUS Business

The grim reality: Many attacks go unreported

Canadian organizations are coming face-to-face with this rapidly growing threat. Ransomware attacks involving personally identifiable information (PII) are considered a breach under the federal Personal Information Protection and Electronic Documents Act (PIPEDA) and similar provincial regulations such as Personal Information Protection Acts (PIPA). Canadian organizations are required to notify regulatory bodies and customers if customer information is breached and poses a significant risk of harm. While some breaches must be reported to the Office of the Privacy Commissioner of Canada (OPC) if there is real risk of significant harm due to the nature of the compromised data, other businesses may choose not to report a breach unless required by law.

Of the organizations that experienced a successful ransomware attack(s) in the last 12 months, 22% did not report it to government authorities. **The Financial Services, Education and Retail sectors are the least likely to report ransomware incidents.**

Did your organization report successful ransomware attacks to regulators or government authorities?



TELUS Business

Why do so many ransomware attacks in Canada go unreported?

Not all ransomware attacks involve customer PII, making risk assessment a "grey area" subject to interpretation. An organization may fail to report an attack for reasons such as:

- Concerns about bad publicity and loss of reputation, or to avoid scrutiny into how it handled a ransomware attack
- Not fully understanding the extent of the breach and the impact on the organization
- Failure to recognize the obligation — and the value to the organization — in reporting the incident
- Prioritizing restoration of business continuity over contacting authorities, especially when the victim is struggling to get back on its feet while curtailing reputational damage
- Avoiding notifying authorities that have proscribed ransoms, because doing so eliminates the easiest and quickest option to restore business operations

However, for the benefit of the wider community, it is important to report ransomware attacks to law enforcement or agencies like the Canadian Centre for Cyber Security. Why? Reporting allows law enforcement officials to conduct "contact tracing," allowing them to better identify threats and trends being seen in the wild and where possible, to support victims with assistance such as free decryption keys.[3]

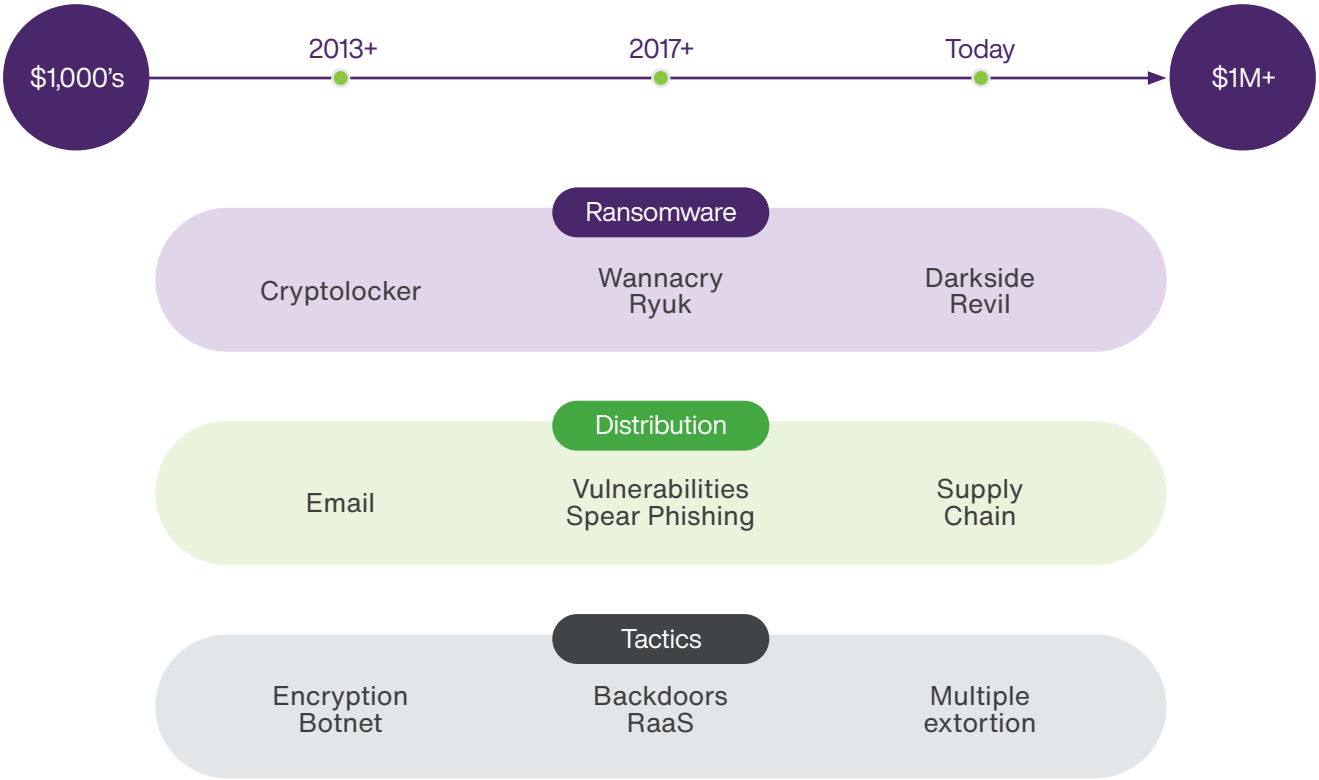
The impact of failing to comply with mandatory reporting requirements can be hefty. Organizations that fail to report data breaches to the Office of the Privacy Commissioner of Canada (OPC) and/or affected individuals or businesses may be subject to court action, regulatory compliance audits initiated by OPC based on victim complaints, and public disclosures that can harm their organizational reputation.

[3] https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099

Ransomware: A continuously evolving adversary

Ransomware has evolved in sophistication at a dizzying pace. Ransomware malware is becoming more advanced, distribution is becoming more targeted, and tactics are continuously evolving to extort the greatest ransom from victims. Attackers are strategic adversaries who perform detailed reconnaissance before launching attacks. They gather information about financials and insurance coverages to gauge the ability of a victim to pay a certain amount.

What does that evolution look like? From the introduction in 2010 of the Bitcoin cryptocurrency, which allows for untraceable payments, to the increasingly sophisticated distribution methods and complex tactics used over time, threat actors have worked hard to ensure that payment of ransom feels like the quickest way out for targeted organizations.



TELUS Business

How is ransomware infiltrating Canadian organizations?

Many organizations continue to struggle with basics like regular patching and vulnerability management. And it's not hard to compound the problem; poor patch and vulnerability management can bring about even greater organizational risk as more digital transformation technologies are introduced. As the numbers demonstrate, threat actors are aware of, and seek out, these cracks in organizational defences.

Knowledge of vulnerabilities, exposures, and associated risks is critical for any organization when establishing threat prevention and detection controls. Without this knowledge, businesses are left with blind spots that threat actors can exploit. **The top three attack vectors in Canada are misconfigurations, email/phishing, and known vulnerabilities.** Smaller organizations are particularly slow to patch known vulnerabilities, and attackers can easily exploit these with readily available off-the-shelf tools.

Rounding out the top six attack vectors are zero-day vulnerabilities, third-party partners, and IT supply chain. These attacks are difficult to detect because the tools for detecting them are not always in place or because the attacks progress from trusted avenues like the IT supply chain or third-party partners.

What is misconfiguration?

This is an incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.[4] Instances of cloud misconfigurations are becoming of greater concern as more organizations make the move to cloud platforms.

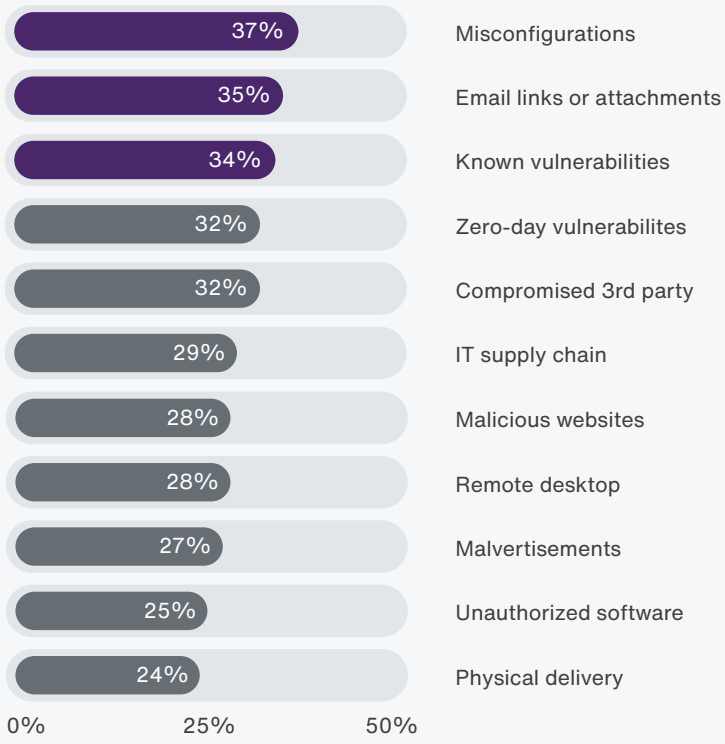
What is zero-day vulnerability?

This is a vulnerability in a hardware system or software that has been disclosed but for which the vendor has not yet issued a patch.

TELUS Business

[4] https://csrc.nist.gov/glossary/term/misconfiguration

Misconfigurations, email/phishing, and known vulnerabilities are the top 3 attack vectors in Canada

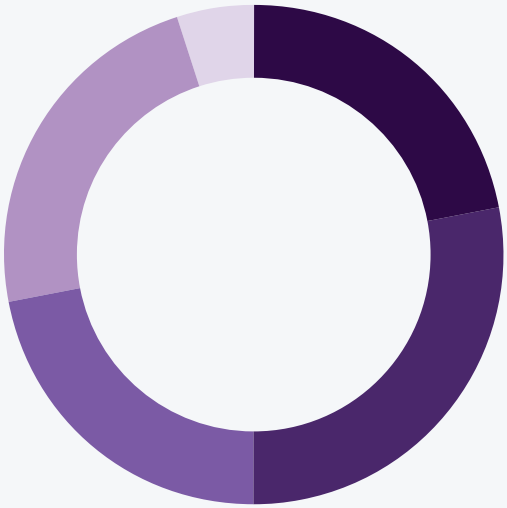


Q: In the past 12 months, which ransomware delivery mechanisms were used in attempted or ransomware attacks?

System and application hardening are critical to shutting down most of these attack vectors. Additionally, a robust vulnerability management program (VMP) is key to finding and closing gaps introduced as a byproduct of changes and/or upgrades within your environment.

Despite the importance of a vulnerability management program, only **50% of Canadian organizations report having a formal program in place**. That leaves the other 50% with blind spots and open vulnerabilities within their environment that adversaries can capitalize upon.

Which statement best describes the current state of your organization's vulnerability management program?



- **22%** We have a formal program that prioritizes vulnerabilities based on organizational risk and orchestrates with IT and security teams for remediation
- **28%** We have a formal program that prioritizes vulnerabilities based on CVSS (Common Vulnerability Scoring System) and orchestrates with IT and Security teams for remediation
- **22%** There is an informal process that priorities vulnerabilities, but remediation is not tracked
- **23%** We have a vulnerability scanning tool that is used ad hoc
- **5%** There is no process for vulnerability scanning

Q: Which statement best describes the current state of your organization's vulnerability management program?

What can be done? To start, organizations must test their IT environments for weaknesses and vulnerabilities to exploitation following any major change or event such as adding new network infrastructure or applications, significant upgrades, establishing new office locations, applying security patches, or updating end-user policies.

Establishing a formal vulnerability management program will help identify gaps and weaknesses using a framework that leverages regular testing. A VMP integrates threat intelligence, continuously monitors for vulnerability and exposures, and dynamically adjusts to the risk associated with them as they are exploited by attackers. Most open vulnerabilities have exploit tools available for adversaries through the ransomware-as-a-service model, so the odds of unpatched vulnerabilities being exploited is very high and must be addressed quickly.

A formal VMP ensures not only that vulnerabilities are found but that they are prioritized, with processes in place to reduce overall risk exposure and prioritization of remediation activities on an ongoing basis. Reducing risk is more than patching the system; it could involve disabling unnecessary services, decommissioning and/or replacing applications and devices, adding additional compensating controls, reducing blast radius/impact, and much more.

As part of a VMP, once vulnerabilities are discovered, remediation efforts should be tracked and prioritized based on business context and threat intelligence. Effective tracking and prioritization can be accomplished via the creation and maintenance of a risk register. This can be used to track discovered vulnerabilities, their priority, and their remediation status. Anything that cannot be patched or remediated upon assessment should be logged and reviewed by management. These steps ensure that gaps can be discovered, prioritized based on associated risk, and either mitigated or accepted by the business.

Despite their clear effectiveness, formal VMPs are found less often in small and medium-sized businesses (SMBs) compared with large enterprises; this is not surprising given that bigger organizations tend to have access to more resources and more robust security processes.

The value of a vulnerability management program is undeniable

63%

of organizations with a VMP did not fall victim to a successful cyberattack

46%

of organizations without a VMP experienced a successful cyberattack

Maintaining a formal vulnerability management program significantly reduces the risk of suffering a ransomware attack

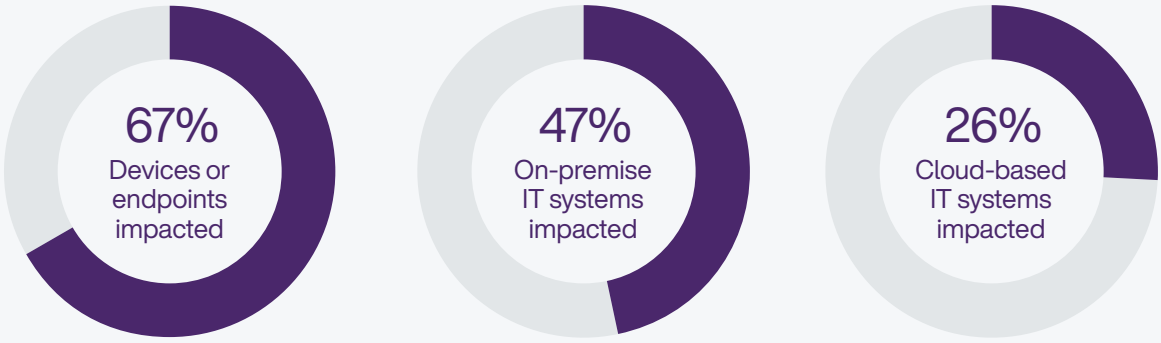
	Zero successful attacks
We have a formal program that prioritizes vulnerabilities based on organizational risk and orchestrates with IT and security teams for remediation	**30%**
We have a formal program that prioritizes vulnerabilities based on Common Vulnerability Scoring System (CVSS) and orchestrates with IT and security teams for remediation	**33%**
There is an informal process that prioritizes vulnerabilities, but remediation is not tracked	**10%**
We have a vulnerability scanning tool that is used ad hoc	**21%**
There is no process for vulnerability scanning	**6%**

Q: Which statement best describes the current state of your organization's vulnerability management program?

Ransomware: Endpoint devices are just the beginning

Unsurprisingly, endpoint devices continue to be the most affected when it comes to damage within IT environments, followed by on-premises IT systems. However, it is important to remember that few attacks are limited to endpoints alone. With many organizations making the move to cloud, threat actors are similarly turning their attention to these new environments.

While endpoints continue to take the brunt of attacks, ransomware designed to target cloud-based systems is on the rise



Q: Which of the following impacts did the most damaging ransomware attack experienced in the last 12 months have on your organization?

TELUS Business

Attacking on-premises IT systems and the cloud

For most respondents, the most damaging attacks affected not only endpoint devices but also on-prem IT systems and cloud resources. These attacks can be especially damaging to SMBs and midmarket organizations where one or two servers are running everything within the environment. The impact of a successful attack on these organizations, with all of their eggs in one technology basket, can be much larger and potentially longer-lasting.

What is RansomCloud?

RansomCloud is a ransomware attack designed specifically to compromise and encrypt data hosted in cloud services.

Ransomware attacks specifically engineered for cloud systems are notably on the rise, such as RansomCloud attacks that target cloud-based services like Office 365. Business continuity is becoming more dependent on cloud-based services like virtual desktop infrastructure (VDI), cloud-based storage, and other components. They host massive amounts of organizational data and are shared by many users, which make cloud services a hot target for adversaries.

More than 1 in 4 respondents indicated they had experienced the compromise of cloud resources. Instances of compromised cloud systems are significantly higher within the Retail and Municipalities verticals: 40% and 36%, respectively.

A new norm: Multiple extortion ransomware

Historically, a robust backup and recovery plan protected organizations against locker and crypto ransomware in most cases. If an attack was successful, organizations had the back-ups needed to restore their data to pre-encrypted state. However, adversaries have responded to improved backup and recovery processes with a new tactic: **multiple extortion**. In these attacks, data is both exfiltrated and encrypted, resulting in victims' being held hostage by adversaries who threaten to publish the exfiltrated data online or inform media and customers.

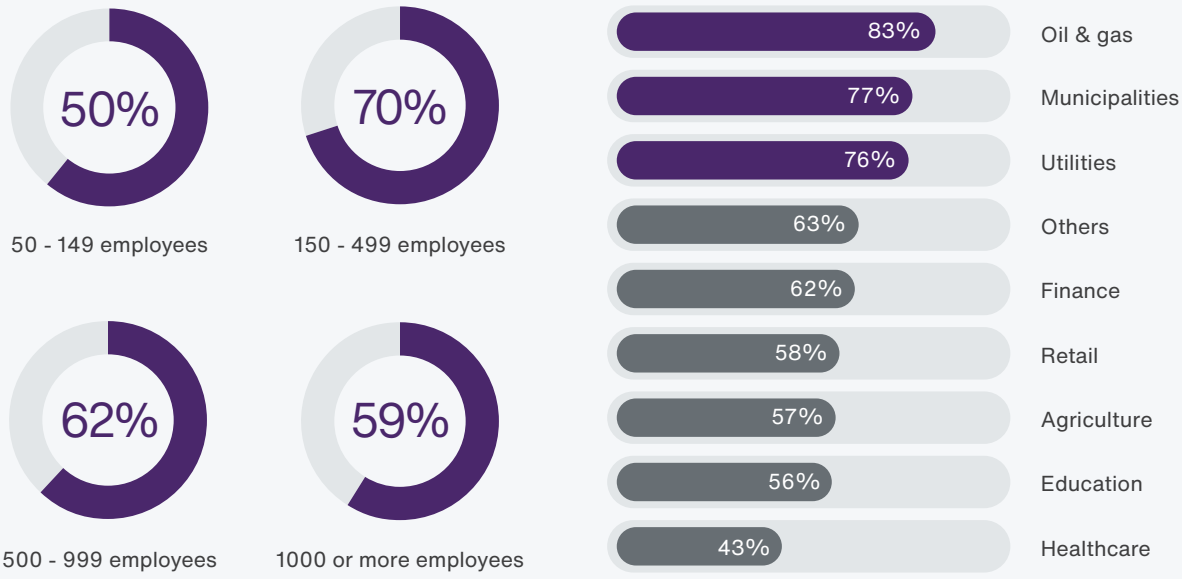
Multiple extortion ransomware has emerged as the most common type of ransomware, with 63% of ransomware attack victims reporting a multiple extortion attack. The industry verticals reporting the highest rate of multiple extortion attacks were Municipalities, Oil and Gas, and Utilities.

What is multiple extortion?

Multiple extortion is a ransomware breach that also results in unauthorized transfer of data by a malware or malicious actor. It can be defined as ransomware plus data exfiltration.

63% of ransomware attack victims report experiencing a multiple extortion attack

Percentage of organizations experiencing multiple extortion



Extortion without encryption

Extorting businesses with their exfiltrated data is proving to be a successful model for many adversaries when compared with monetizing that data on the dark web. Cyberthreat groups like SnapMC have abandoned encryption altogether and are focusing only on exfiltrating data.[5] In instances of pure extortion, the payment of ransom provides little guarantee to victims, as there is no way to confirm with confidence that threat actors have not copied the compromised data for further exploitation in the future.

TELUS Business

[5] https://research.nccgroup.com/2021/10/11/snapmc-skips-ransomware-steals-data/

Reinfection after recovery

Lightning can strike twice when it comes to ransomware: **15% of Canadian organizations that suffered a ransomware incident indicated that they were reinfected by the same ransomware attack after recovery**. This highlights the importance of creating and following an in-depth response plan, designed to ensure that all traces of infection are removed from the compromised environment. Focusing recovery efforts on the obvious symptoms of an attack alone leaves the door open for reinfection.

A detailed forensic investigation and ongoing vulnerability assessments can identify vulnerabilities or misconfigurations exploited by adversaries. It can also uncover any back doors or malicious code left by adversaries, which are often sold to other attackers on the dark web.

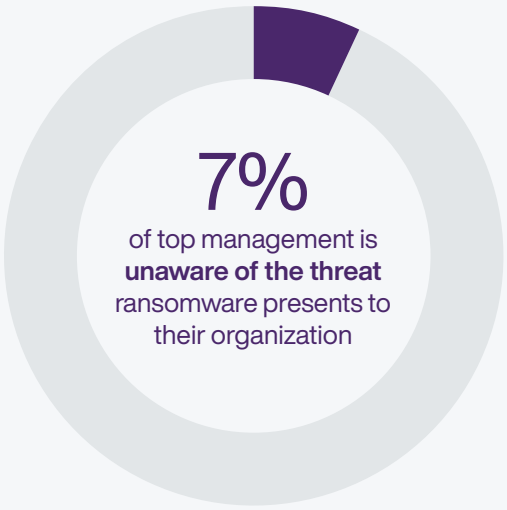
Organizations that upgrade legacy systems and software, maintain a vulnerability management program, adhere to a patching policy, conduct security awareness training, and engage third party security services reduce their reinfection rate by half. Only 9% of organizations that conducted these initiatives were reinfected by the same ransomware attack, compared with 20% that conducted only one of the initiatives.

> Organizations that upgrade legacy systems and software, maintain a vulnerability management program, adhere to a patching policy, conduct security awareness training, and engage third party security services **reduce their reinfection rate by half**.

Don’t wait for a ransomware attack to improve protection

After suffering a ransomware attack, many organizations increase foundational cybersecurity investments in areas such as security advisory and assessment services, identity and access management, end-to-end asset visibility and control, and new cybersecurity tools and technologies. However, forward-thinking organizations are recognizing that ransomware attacks are a matter of “when,” not “if,” and are embarking on a path of proactive security modernization before a breach occurs. An effective cybersecurity strategy is much more protective than “putting out fires” after the fact.

An important first step in empowering IT teams to proactively mature an organization’s security posture is obtaining buy-in from board members and senior leadership. Yet only **32% of respondents indicated that senior leadership had discussed the threat of ransomware recently, with 7% reporting that their top management is unaware of the threat posed by ransomware to their organizations**. This data highlights that obtaining meaningful buy-in may require cybersecurity education, to give decision makers a deeper understanding of the threats their organization is facing.



So, how can you create awareness with board members and senior leadership about a problem some don't even know exists? Conducting regular tabletop exercises is an effective tool that can help boost awareness by providing a simulated experience of a breach in real time. These exercises quickly highlight gaps in both processes and protections and demonstrate the impact of not being proactive in the event of a real incident.

Defence-in-depth: Prevention and monitoring

Attackers are continuously developing new TTPs, so even multilayered security controls may fail sometimes due to newly discovered vulnerabilities, outdated rules (e.g., firewall, SIEM), and new threats.

Monitoring is key to quickly detecting the threats that bypass security controls; 24 x 7 monitoring and intelligence-based threat detection are critical for enabling security teams to act quickly. Canadian organizations often face skills shortages and budgetary constraints to maintain this level of monitoring. Due to this, **only 38% of organizations invest in active, 24 x 7 monitoring of their environments**. The rest are left to manage this gap with on-call staff which can result in slower response times.

A solution to this is investing in orchestration and automation tools which can launch coordinated and automated incident responses based on predefined playbooks that take effect the moment threats are detected. This can result in reduced dwell time for attackers and a greater likelihood of preventing damage. Alternatively, security services providers can help fill the gap, with services that provide the 24 x 7 monitoring and response services organizations need.

Finding ransomware with intelligence-based detection

Clearly, there are massive gaps in ransomware detection; **almost one third of Canadian organizations surveyed had instances of ransomware that were initially detected outside of IT and Security** (internal staff, customers, and/or partners).

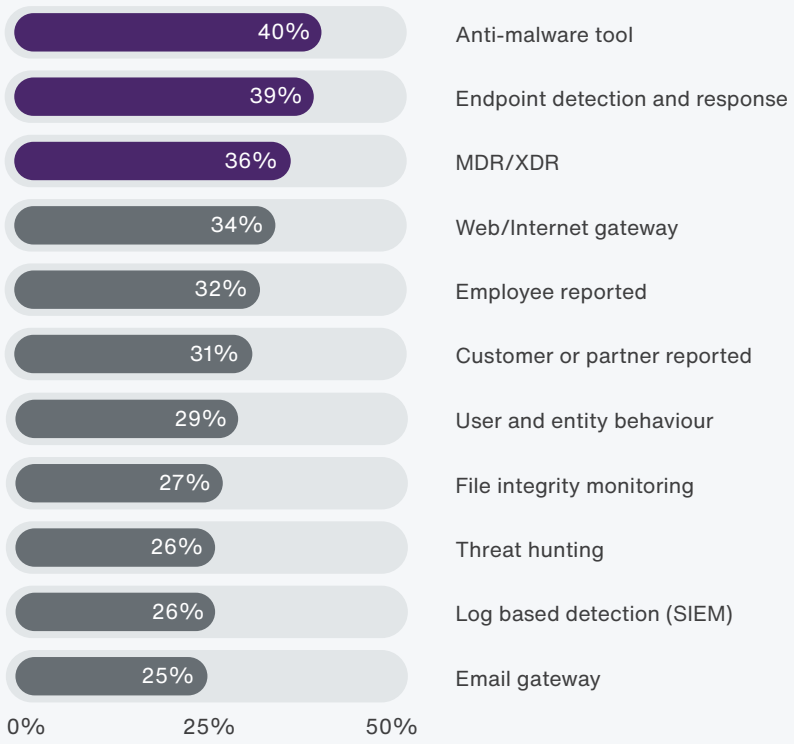
The Retail (45%) and Utilities (50%) verticals had the most instances of ransomware infections that were undetected by IT and were communicated by a customer or partner.

Intelligence-based detection is seen as more effective than traditional log-based detection. TTPs are continuously evolving, and zero-day attacks are among the top four vectors, meaning that rule-based or signature-based detection may be inadequate. Furthermore, ransomware attacks are not confined to endpoints but increasingly affect on-prem IT systems and cloud resources, which demand advanced detection.

Organizations generate immense amounts of data, network and endpoint telemetry, and, depending on the nature of their business, specialized IoT data produced by Industrial Internet of Things (IoT) and Internet of Medical Things (IoMT) devices, which can be utilized for threat detection. Tools like Managed Detection and Response (MDR) are critical for extending threat detection across the environment and providing 24 x 7 monitoring with artificial intelligence (AI) and machine learning (ML)-based detection and triage to launch a quick and coordinated response.

The survey data shows that many Canadian organizations see the value of more robust, 24 x 7 detection and response solutions and are adopting more modern tools like Endpoint Detection and Response (39%) and MDR (36%).

Endpoint protection and MDR tools are imperative to proactively detecting ransomware attacks



Q: In the past 12 months, by which methods were ransomware attacks first detected?

Ransom - you don't always get what you pay for

Your organization has been hit by a ransomware attack. Now what? By paying the ransom, you could be funding your adversaries and encouraging future attacks. Evaluating ransom payment and non-payment options is a complicated process that involves multiple stakeholders including leadership teams, legal counsel, recovery teams, incident response teams, and other IT functions.

This evaluation process goes beyond the organization's response preparedness, incident response retainers in place, or cyber insurance. There are long-term repercussions from both an ethics and a business perspective that must be considered. Organizations that have invested years of work in building a brand in the industry may resist being perceived as weak or surrendering to the demands of adversaries. They may also question the ethics of paying a group that will go on to extort others using those funds.

From a business perspective, weighing the potential disruption of services, financial impact, or inability to restore from backups against the legal implications and business policy makes the decision about whether to pay the ransom a very complex one.

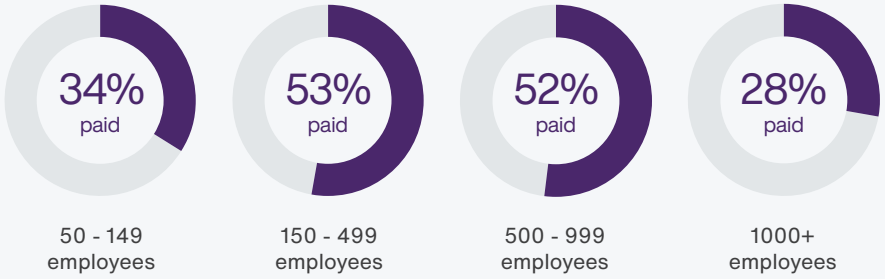
To pay or not to pay

When asked if they did or did not pay ransom after their organization experienced a ransomware incident, 35% of respondents preferred not to say. However,

- Of the respondents who were willing to answer the question, **44% indicated that they did pay the ransom**. Adversaries would view this as a very encouraging payment probability.
- More than 50% of medium (150–499 employees) and large (500–999 employees) organizations indicated that they had paid ransoms to restore their data.

44%

of respondents (that were comfortable sharing) indicated that they did pay the ransom



Q: Has your organization ever paid off the perpetrators of ransomware attacks?

How likely is your organization to pay ransom to the perpetrators of ransomware attacks?

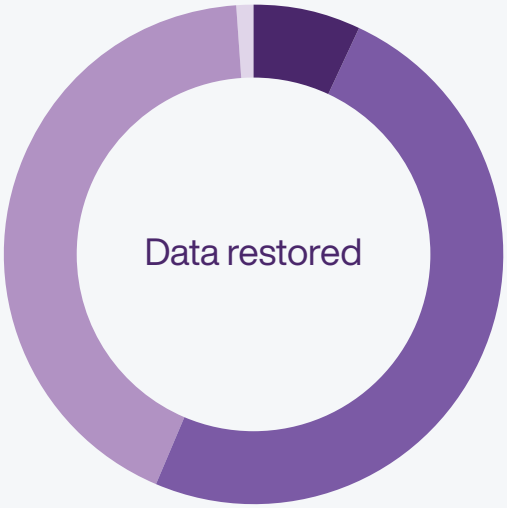
Real-world experience is the key differentiator when answering this question and may indicate overconfidence. **Of those who have not experienced a ransomware incident, 60% indicated they are unlikely to pay ransom. However, for those who have experienced ransomware, only 36% decided to not pay.**

Paying ransom does not guarantee data restoration

Most important, of the organizations that paid ransom, only 42% experienced a full restoration of their data. Furthermore:

- Forty-nine percent of respondents indicate that their data was only partially restored, which resulted in additional costs for unrecovered data.
- For 8% of respondents, the transaction outcome was far from expected. Not only was their data not restored, the hacker also demanded more money to restore data access.

Despite payment, access to data was not restored for more than half of ransomware victims



7%	Data was not restored
49%	Data was partially restored
42%	Data was completely restored
1%	Attackers demanded more money to restore data access

Q: What was the outcome experienced after the last ransom payment was made?

Ransom payment is not a fair transaction for victims, since the attacker has no obligations or accountability and holds all of the power. It is not surprising that 37% of respondents who did not pay ransom chose that route because their organizations were concerned that they could not trust hackers to engage in fair trade.

While most attention in the media tends to focus on payment (or non-payment) and the amount paid, rarely are the outcomes of payment discussed. Understandably, most organizations are hesitant to admit they weren't made whole despite capitulating to ransom demands, but it is important to recognize what the data demonstrates - payment is far from a guaranteed ransomware recovery strategy.

Negotiating may make things worse

Negotiating ransom may reduce the ransom amounts, but it significantly impacts the odds of having data successfully restored. Of the organizations that paid ransom, 49% indicated that they did not pay the full amount but negotiated it down. However,

- **Fifty-five percent of organizations that paid the full ransom received full data restoration.**
- **Thirty-two percent of organizations that negotiated the ransom received full data restoration.**

The attack doesn't end with paying the ransom

A ransomware attack may not end with the payment of ransom, the restoration of data, and the resumption of your business operations. Unfortunately, 15% of Canadian organizations who suffered a successful ransomware attack report that they were reinfected by the same ransomware after recovery.

The other problem is that 63% of the organizations that experienced ransomware incidents were subjected to multiple extortion, which expands the organization's worries far beyond data restoration. When this happens, an organization is forced to invest substantial resources to communicate the data breach to customers and partners, monitor the dark web for exfiltrated data, and perform extended remediation based on the type of data that was exfiltrated.

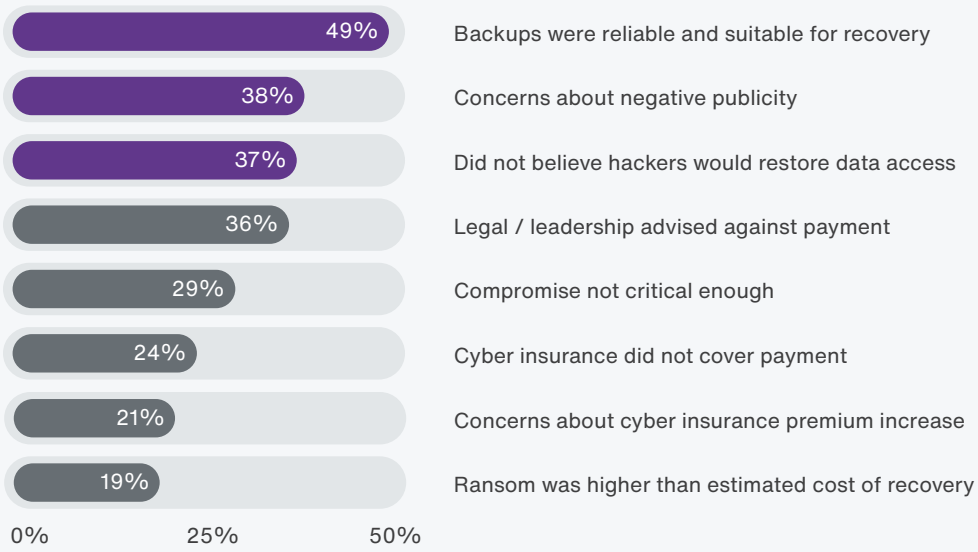
This mixed bag of outcomes is one of the reasons Canadian organizations may decide not to pay the perpetrators.

Why ransoms are not paid

Of the respondents who reported that their organizations did not pay ransom, several key deciding factors emerged:

- **Faith in backups:** Forty-nine percent stated that the top reason for not engaging the adversaries was high confidence levels in backups.
- **Bad publicity:** Thirty-eight percent considered not paying because it would have led to bad publicity, especially within large organizations with more than 1,000 employees, where negative publicity and lack of trust in engaging with the hackers were top concerns.
- **Industry:** Industry verticals have specific concerns when evaluating whether or not to pay the ransom. For example:
    - In Healthcare and Financial Services (FS), 69% of healthcare respondents and 56% of FS respondents indicated that their key reason for not paying ransom was that the leadership/legal team advised against it.
    - For Municipalities, 75% of respondents indicated that bad publicity was the key reason they decided not to pay ransom.

What were the main reasons that ransom was not paid?

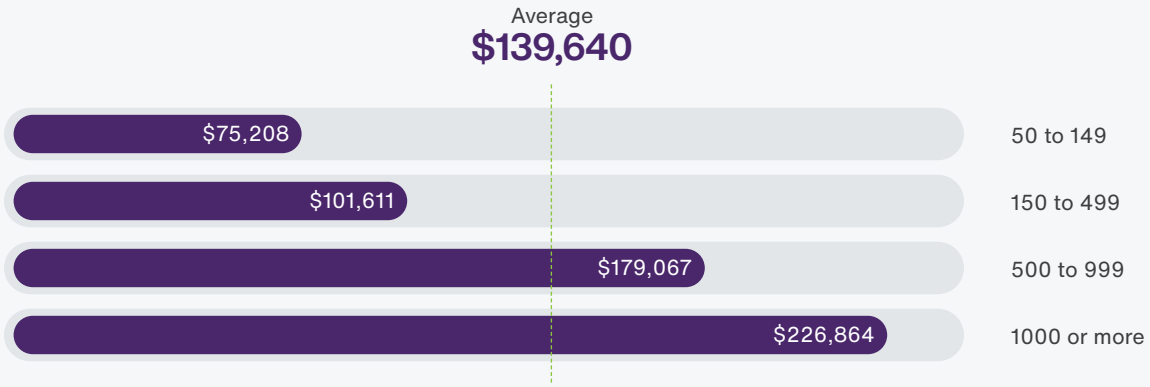


Ransom amounts paid by Canadian organizations

The average ransom paid by Canadian organizations is $140,000 per attack, with significantly more ransom paid by larger organizations. The highest ransoms were paid for crypto ransomware. These are often elaborate, targeted, and sophisticated attacks that may disrupt business operations, while the focus of multiple extortion is predominantly on exfiltrating data quickly, often with unsophisticated attacks.

TELUS Business

On average, ransom payment will cost organizations **$140,000**



Q: What was the amount of the last ransom paid?

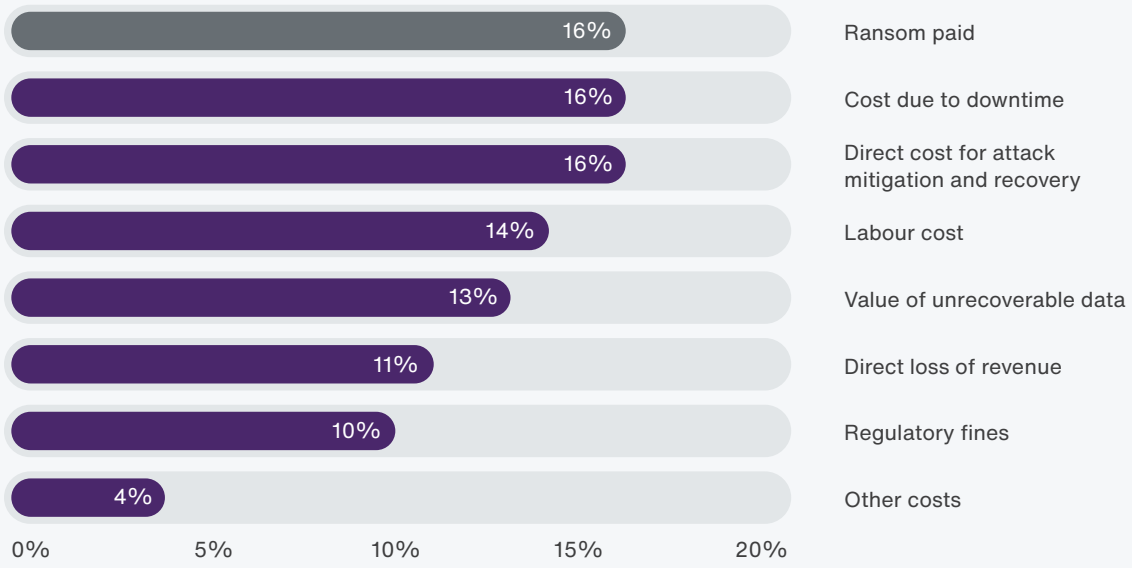
Beyond payment: the additional impacts of ransomware

Ransom payment amounts always make headlines, but those who have been affected know that the real cost of ransomware is far greater than just the ransom paid.

According to survey respondents, the costs associated with downtime account for an average of 16% of the total direct cost of the incident. This is much worse for industries like Financial Services, where downtime accounts for an average 22% of the direct costs incurred.

Attack mitigation and recovery may involve extensive participation of external experts, overtime for internal resources, and specialized tools that add to the direct cost of mitigation. On average, mitigation costs account for 16% of direct costs incurred.

Beyond ransom payment, the other costly impacts of an incident



Q: What proportion of the total direct costs of successful ransomware attacks were in each of these categories?

As noted previously, only 42% of organizations that paid ransom received full recovery of their data. The value of that unrecoverable data represents, on average, 13% of overall direct costs. However, its share is substantially higher for industries like Healthcare, where the value of unrecoverable data accounts for an average of 17% of direct costs.

Considering these direct costs, the total cost per ransomware incident escalates quite rapidly and can run into the millions of dollars. Using the chart above to account for the total cost of a significant incident and assuming ransom is paid, we can extrapolate that the average cost of an incident for Canadian organizations varies from an average of $500,000 for small organizations to $1.5 million for larger organizations.

The real cost of ransomware - your organization's future

Ransomware attacks have far-reaching implications that go well beyond the direct monetary cost of decrypting and restoring data. Often referred to as "soft costs," the effects of a ransomware attack on brand reputation and customer impact are difficult to quantify — but they can be enormous.

Ransomware attacks directly impact an organization's growth plans and can derail the adoption of digital transformation (DX) technologies. For some companies, recovery could take a long time and could involve rebuilding systems from the ground up or undertaking massive re-architecting initiatives.

Derailing the journey to digital transformation

Increased focus on DX has led to a sharp uptick in the use of technology to enable contactless customer engagement, remote employee collaboration, technology-led operational rationalization, and new digitally augmented business models and revenue streams. As per the IDC Worldwide CEO Survey, Canadian businesses anticipate 48% of their overall revenue to come from digital products, services, and/or experiences in 2025, up from 30% in 2020.

By 2025 nearly 50% of revenue will come from digital products

Q: What percentage of your revenue do you expect to come from digital products, services, and/or experiences in 2020, 2022 and 2025? (mean summary)

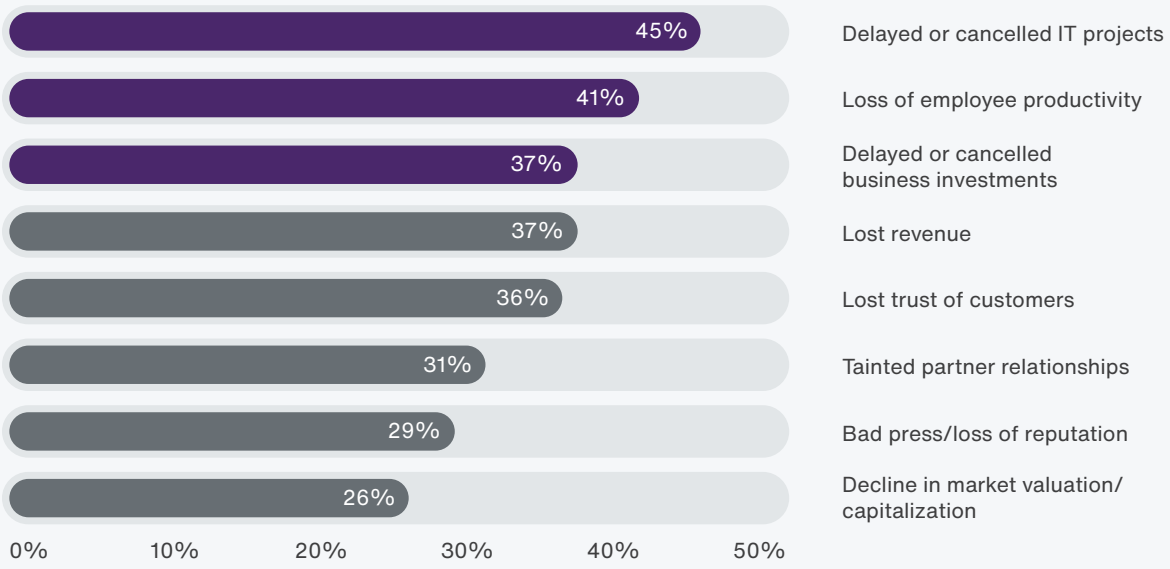
Source: IDC Worldwide CEO Survey, February 2020

A ransomware attack can plunge an organization into a long, tedious process of mitigation and recovery that involves reassessing security architecture, deploying additional tools and technologies, or even re-architecting followed by a reassessment of the new environment.

TELUS Business

As the graph below shows, this process can set organizations back for years by requiring capital that otherwise would have been invested in IT projects or business investments to be redirected to ransomware recovery. This could mean the delay or cancellation of planned adoption of cloud services, IoT, edge computing, analytics, and other innovation accelerators, which are critical to the success of a modern enterprise. This might have been manageable a decade ago, when technology was a driver for operational efficiency, but in today's hyper-competitive market, where technology drives competitive advantage, this could set an organization behind its competitors and cost them future market share.

Ransomware incidents can cost you the future of your business



Q: Which of the following were significantly impacted as a result of ransomware attacks in the past 12 months?

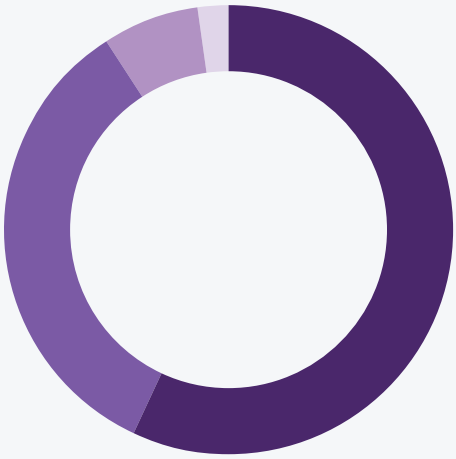
Can organizations really take the risk of being vulnerable? Imagine the effect across industries:

- Banks suspending digital banking services
- Retail organizations with compromised ecommerce systems
- Universities no longer offering virtual classrooms
- Medical services suspended as hackers take over healthcare IT systems
- Assembly lines at a standstill as hackers infiltrate manufacturing operations
- Municipalities suspending online citizen services, limiting emergency responders / dispatch services or stalled tax payments
- Agriculture, utilities, and oil and gas companies losing control of their OT systems to hackers, resulting in shortages or service disruptions

Too often ransomware response falls short

Ransomware infections can create a state of emergency within an organization. For those without an updated and tested response plan, the situation could lead to total chaos. Building a bridge as you cross the river is not a great strategy when your organization's future is at stake. Time is of the essence. Given the clear importance of an up-to-date incident response plan, it was surprising to see that **only 57% of Canadian organizations periodically update and test their ransomware response plan**.

Only 57% of Canadian organizations periodically update and test their ransomware response plan



- **57%** Yes, and it is periodically tested and updated
- **34%** Yes, it is periodially updated but not tested
- **7%** Yes, but not tested or updated in the last 12 months
- **2%** We don't have a ransomware response plan

Q: Does your organization have a ransomware response plan?

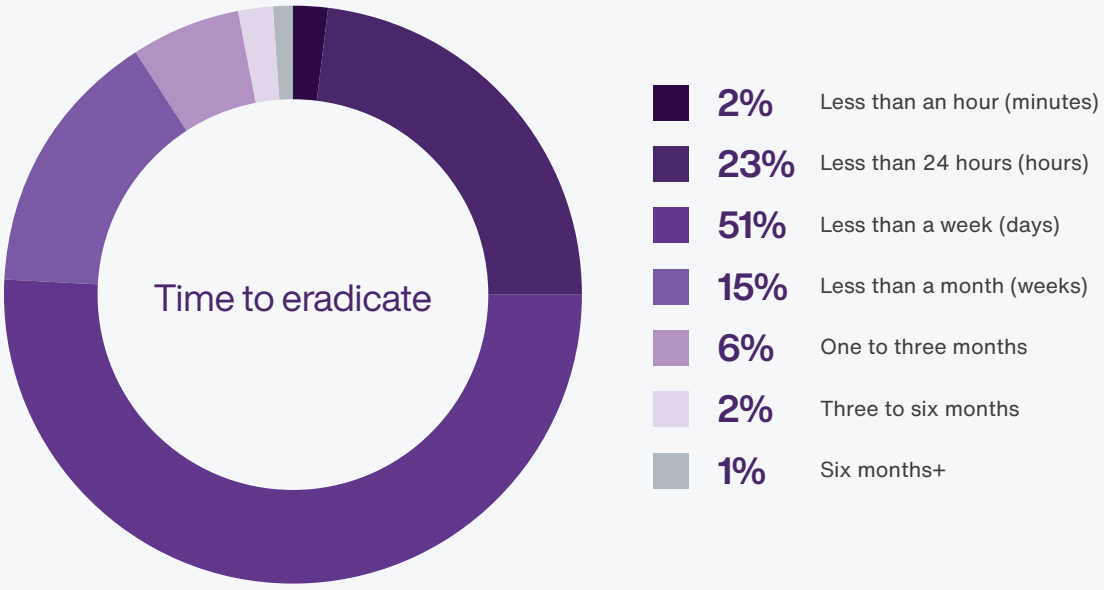
Empower your team to quickly respond and limit damage with an up-to-date response plan

Considering the rate at which adversaries are evolving their Tactics, Techniques and Procedures (TTP), any response plan that is not updated and tested regularly will fall short. The pandemic has accelerated the pace of DX with the adoption of remote work and hybrid IT, causing response plans to lose relevance even faster. Unless response plans are updated continuously and tested frequently, bottlenecks will occur and security teams will find it difficult to contain and eradicate an attack, initiate internal and external breach communication, and initiate recovery.

According to the survey, **organizations with an updated and tested response plan are over 2x more likely to contain and eradicate an incident within 24 hours compared to those that only update without periodic testing.**

Having an up-to-date response plan could make the difference between maintaining an organization's reputation and facing significant negative publicity.

How much time did it take your organization to contain and eradicate the last successful ransomware attack after it was detected?



TELUS Business

Speed is critical when responding to a ransomware incident

When responding to a ransomware incident, the majority of Canadian organizations indicated a response time of a few days: 51% of organizations said they take more than one day but less than a week to effectively contain and eradicate an attack. It is worth noting that 22% of organizations measured ransomware response time in weeks and months.

Interestingly, when asked to estimate how much time it would take to contain and eradicate a ransomware incident after it was first detected:

- **Forty-five percent of respondents who did not experience a successful attack believed that their response time would be less than a day.**
- **Only 25% of respondents who did experience a ransomware incident indicated response times of a day or less.**

Clearly, overconfidence is a mistake. It is better to be prepared with a ransomware response plan that is continuously updated and tested.

While many organizations may be able to identify and remove a threat actor presence, identify the compromised accounts/software/areas of the network, take the necessary steps to contain the affected elements and conduct a forensic investigation, fully restoring the impacted parts of your network may take much longer.

The slower the response, the higher the risk

A slow response could lead to lateral movement and other systems' being compromised because it gives intruders enough time to compromise backups and exfiltrate and encrypt data. Furthermore, slow investigations can alert hackers, giving them enough time to:

- Cover their tracks and destroy evidence
- Stop the attack temporarily and initiate persistence (deploy a back door or steal passwords) for future attacks

Per survey respondents, response time varies according to the devices and systems that are attacked. For 86% of respondents, the ransomware attack infected only endpoint devices, and those attacks were contained and eradicated within a week. However when attacks extend into other on-prem IT systems or cloud systems, response times grow to beyond a week.

What causes delays in response time?

The first step in almost every ransomware response is defining the scope of the attack before cascading delays affect the recovery process. **For more than 50% of respondents, containing the attack, launching a quick coordinated response, and conducting an effective root cause analysis are the top response challenges.** Lack of orchestration, for example, forces an analyst to toggle between multiple screens and dashboards to investigate and respond to an attack.

An effective **root cause analysis** is critical to identifying the TTP used by adversaries, containing the attack, eradicating ransomware from infected systems, and launching a quick, coordinated response. It identifies which systems were attacked and how much data was affected. Was it a single server or single virtual bucket, or an entire datacentre or cloud environment? Getting answers to these questions will determine the next stage of incident response. Security orchestration and automation (SOA) tools can query other organizational systems, conduct threat intelligence, and enrich alerts for effective root cause analysis and visualization.

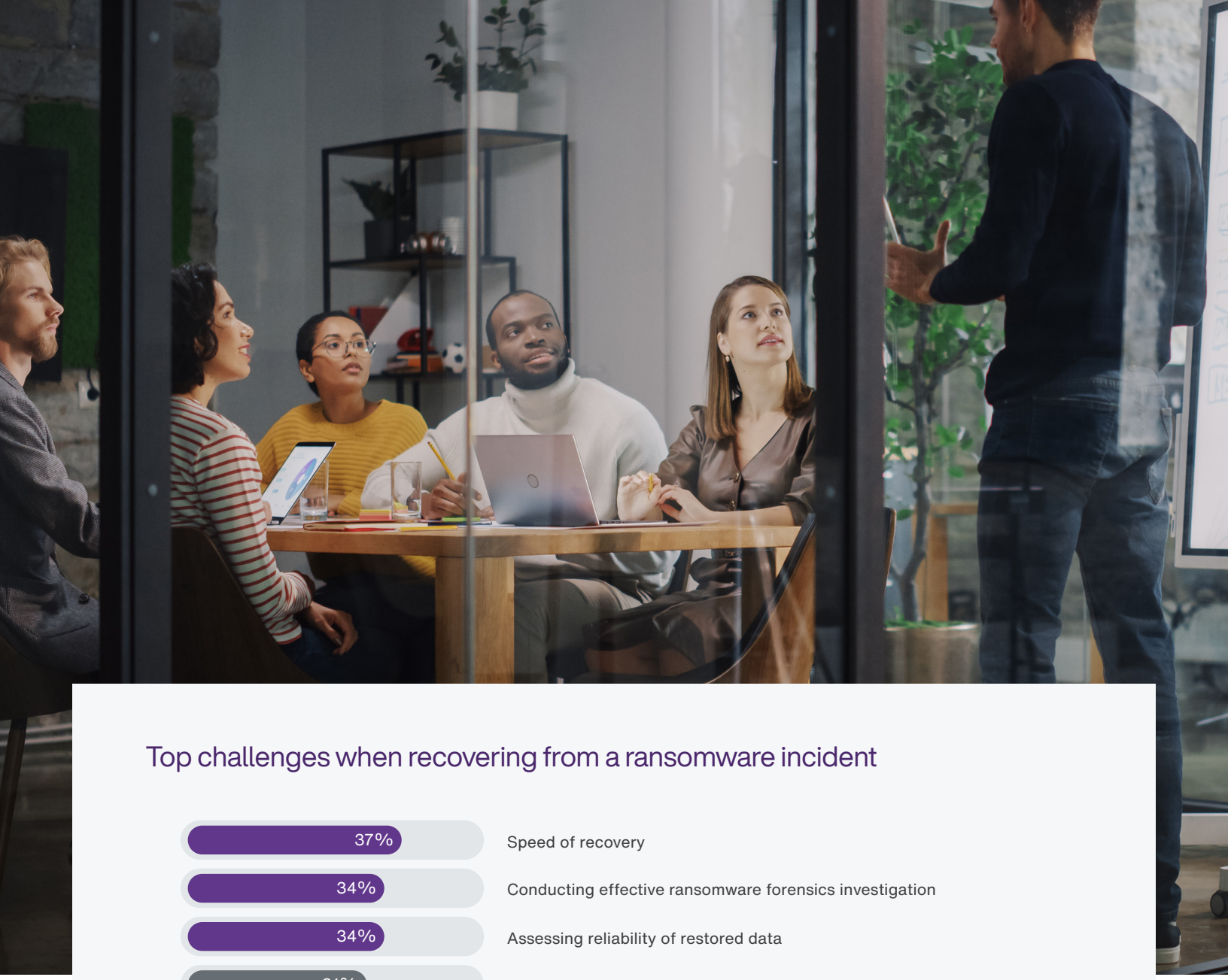
An **automated response** is critical to containing the attack. Creating consistent and repeatable threat response playbooks can automate many steps of the workflows that, without human intervention, can perform activities like isolating a network or host, forcing password resets, and updating firewall rules.

Some ransomware incidents will require advanced response capabilities, and organizations must ensure that they have those skill sets in-house or readily available from external providers.

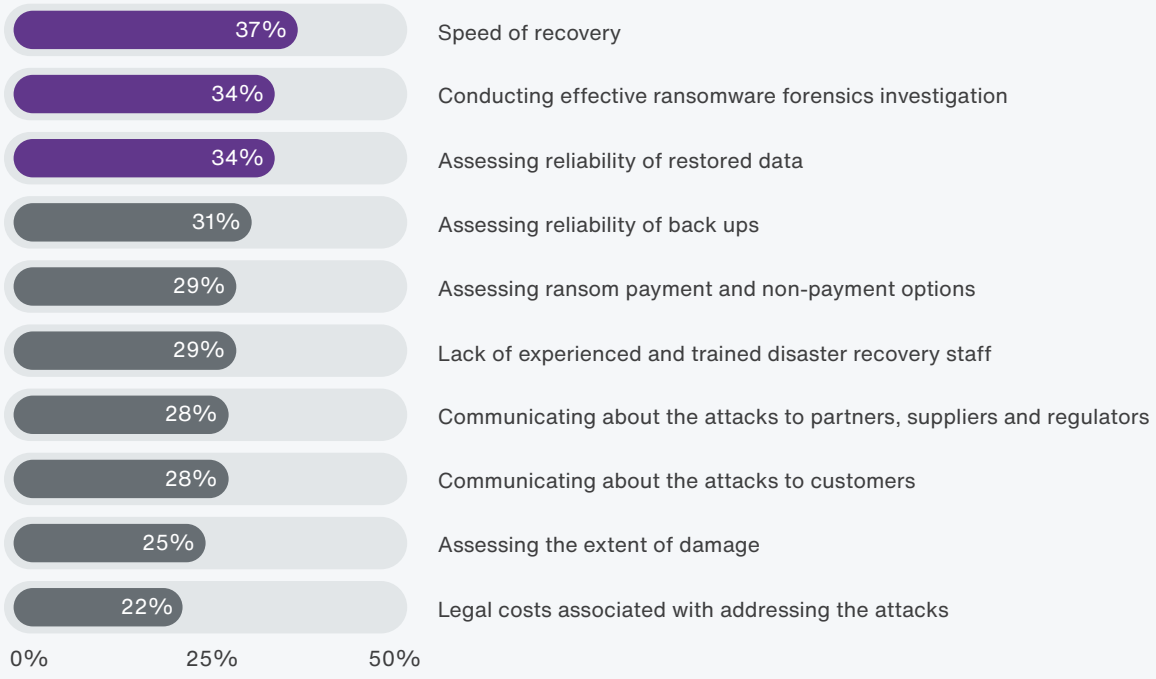
Top challenges in recovering from a ransomware attack

Speed of recovery, forensic investigation, and assessing the reliability of backup and restored data are the top challenges reported by Canadian organizations.

- **Speed of recovery:** Organizations have invested in encrypted, immutable, and air-gapped backups, but these can severely impact recovery speeds.
- **Conducting a forensic investigation:** This is a challenge for Canadian organizations because adversaries employ encryption, covert storage, and communication channels to avoid detection, making the investigation more complicated. Organizations can also encounter internal skills shortages in forensic investigations, which can span multiple areas such as email forensics, database forensics, or malware forensics.
- **Assessing reliability of backup and restored data:** Malware and ransomware programs may go undetected on the target system for days, weeks, or months, making it quite likely that the malware will be backed up along with the regular backups. Upon data recovery, the malware will be written to reinfect the system. This is why assessing the reliability of backup and restored data is among the top challenges for organizations, and must go hand in hand with efforts to protect the organization from ransomware attacks.



Top challenges when recovering from a ransomware incident



Q: What were the top challenges faced by your organization in recovering from ransomware incidents that you experienced in the last 12 months?

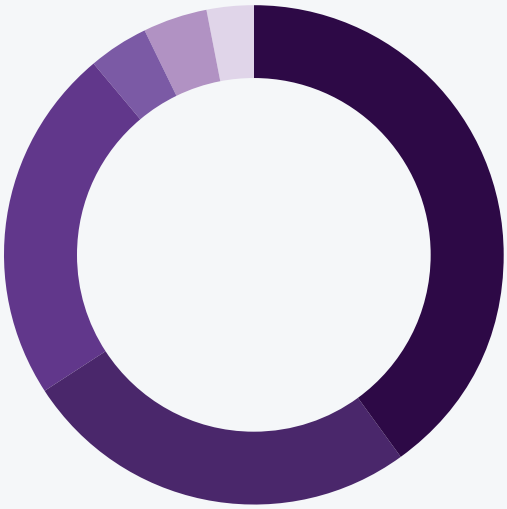
TELUS Business

Cyber insurance: Too good to be true?

Cyber insurance has become an increasingly popular tool for managing ransomware risk. It can cover monetary losses such as ransom, downtime, and regulatory fines. However, some would argue that cyber insurance fuels the ransomware industry, because companies relying on insurance to cover cyberattacks may fail to adopt the security measures needed to prevent such attacks in the first place. A balanced approach is needed.

The financial cushion provided by cyber insurance results in economies around the world provisioning for ransomware financially, leaving the threat uncontested — and the ransomware industry free to grow and build new business models.

Has your organization considered purchasing cyber insurance for ransomware?



- **40%** Currently have cyber-insurance
- **26%** Had cyber-insurance but no longer have coverage
- **23%** Considering now but no decision yet
- **4%** Considered and decided not to purchase
- **4%** Have not considered cyber-insurance
- **3%** Not sure

Adoption of cyber insurance by Canadian organizations

Cyber insurance is an evolving industry and far from a common standard. However, with cyberattacks on the rise, there is an acute surge in demand, and cyber insurance providers can practically choose their customers, policy exceptions, sub limits, escape clauses, and security requirements. There is also some evidence that insurance providers are electing to make changes over which organizations have no control, including, "*increased premiums (reported by 35%), requests for new forms of proof/verification of cybersecurity measures being in place (34%), and changed eligibility requirements for obtaining/renewing coverage (29%). About one quarter also reported reduced reimbursement amounts for ransomware attacks.*"[6]

Despite this, **40% of Canadian organizations indicated that they currently have cyber insurance that covers ransomware attacks**. Digging a little deeper, we see that:

- Organizations that have experienced ransomware attacks in the last 12 months are more likely to have cyber insurance.
- Fifty percent of organizations that suffered four or more attacks are currently covered by cyber insurance, while 27% of these had insurance previously but no longer have coverage.
- Overall, 26% of organizations were covered in the past but do not have coverage now, while 23% are considering buying cyber insurance.

Cyber insurance often falls short

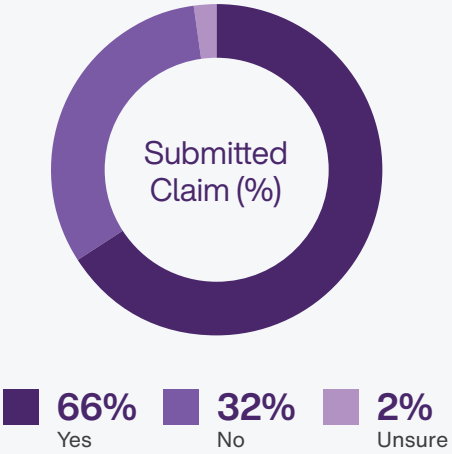
Cyber insurance as a ransomware risk management tool is less effective than a preventative approach. In the last 12 months, 66% of Canadian organizations with cyber insurance have submitted a claim for ransomware attacks. Of these:

- Seventy-nine percent of organizations that filed a claim received a payout, but coverage for 28% of them was dropped.
- Eight percent did not receive any payout at all, and a further 9% are still waiting for a payout.

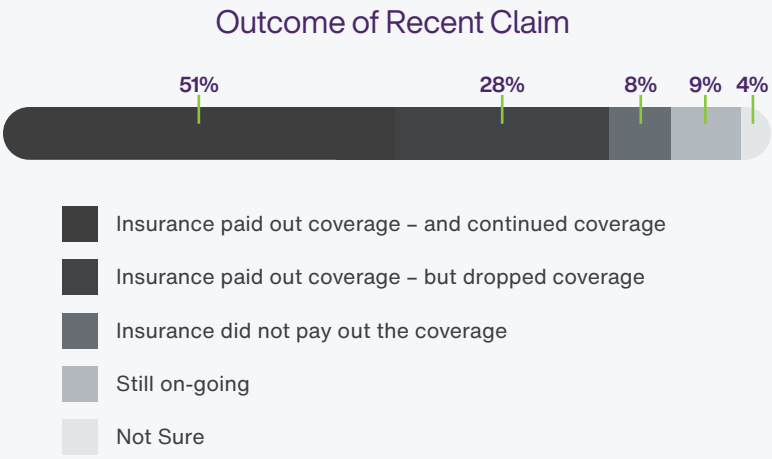
In Canada alone, "*almost **two thirds** of cybersecurity professionals support legislation that would prohibit ransom payments.*"[7]

[6] https://www.cira.ca/blog/cybersecurity/cybersecurity-insurance-canada-2021
[7] https://www.cira.ca/blog/cybersecurity/should-ransomware-payments-be-illegal-canada

40% of Canadian organizations have cyber insurance that covers ransomware attacks



Q: Has your organization ever put in a claim for cyber-insurance from a ransomware attack?



Q: What was the outcome for the most recent cyber-insurance claim for a Ransomware Attack?

The bottom line? The cyber insurance industry is new and continues to evolve. Besides the reality that payouts may be less than expected and coverage difficult to maintain after a claim, we are seeing a shift toward less tolerance of ransomware payments, with some governments exploring legislation to outlaw the payment of ransom and finding new ways to support ransomware victims to further deter payment.

Start with a solid foundation: Ransomware defence strategies

Regardless of the size of an organization or the maturity of its posture, facing a threat as persistent and pervasive as ransomware can be daunting, and it can be hard to know how to best protect yourself. The TELUS Cyber Defence Centre has outlined the following key elements of a multilayered ransomware defence strategy.

Formalize your vulnerability management program. It's impossible to know where the gaps are unless you take the time to find them. Implementing a formal program will ensure that you are equipped to find, prioritize, track, and address gaps and remain prepared to stay on top of vulnerabilities, today and over time.

Review your incident response plan. At least once a year, review all associated policies, processes, identified stakeholders, communications workflows, incident definitions and playbooks and update as necessary. Additionally, be sure to test your IR playbooks via regular tabletop exercises to ensure employees understand the role they have to play during an incident.

Leverage a layered suite of ransomware defence controls:

- **Strong email filtering:** This is a key protection, since phishing continues to be a major ransomware vector.
- **Endpoint protection:** The more endpoints you have, the larger your threat surface becomes. With many organizations leveraging a hybrid work model, the additional security controls and capabilities that endpoint protection can provide are an important proactive protection tool.
- **24 x 7 monitoring and response:** Threat actors operate 24 x 7, and so should your monitoring and response capabilities. Introducing solutions like Managed Detection and Response ensures your environment is monitored around the clock and that a swift, automated response is taken when threats are detected, giving your organization peace of mind.
- **Security awareness training:** Educated users are a valuable extra layer of defence. Be sure they are prepared by creating a strong culture of security where everyone understands the role they have to play in keeping themselves and the organization secure. Evolve your program as your users become more adept at spotting and reporting threats.

Consider subscribing to a **threat intelligence monitoring** service to increase your visibility into the threat landscape. Proactively subscribing to this kind of service enables your organization to find sensitive data threat actors may use to access your network, like compromised credentials for sale on the dark web. This visibility empowers your team to address the risk before it can impact your organization.

For existing platforms and applications, enable **multi-factor authentication (MFA)** wherever possible and ensure they are regularly backed up and tested.

Don't set it and forget it. Each of the controls listed above requires ongoing management, but that can be challenging if you don't have the needed resources at your disposal. Working with a cybersecurity partner can alleviate this pressure from your IT and security teams, allowing them to focus on other priorities while still ensuring you're getting the comprehensive protection you need.

About the TELUS Cyber Defence Centre

The TELUS Cyber Defence Centre (CDC) is the hub for cybersecurity operational and threat intelligence activities. It is home to the Incident Response and Security Operations Centre teams, who collaboratively work to defend customers as well as TELUS data and systems, using the latest orchestration, automation, detection and response tools. The Threat Intelligence team tracks the latest cyber threats and trends, leveraging our unique viewpoint as a national telecommunications service provider and cybersecurity partner to hundreds of Canadian organizations. The CDC also serves as the focal point for our external partnerships with industry leaders and national stakeholders to exchange and provide actionable threat intelligence.

About TELUS

At TELUS, we are committed to using our world-leading technology to create meaningful change. By reinvesting 5 percent of our profits back into our communities, connecting Canadians in need and committing to become a zero-waste, carbon neutral company by 2030, we hope to make the world a better place. To help make cybersecurity more accessible, we established TELUS Wise, a free digital literacy education program that offers workshops and resources to help Canadians of all ages stay safe in a digital world.

As a cybersecurity leader and national telecommunications service provider, TELUS is well positioned to offer a unique perspective on the security threats and trends businesses face today. We leverage our 20+ years of experience securing our own employees, national network, and customers across Canada to help organizations achieve their desired security outcomes. We are one of five companies in Canada (and the only telecommunications and security provider) to have secured the “Global Privacy and Security by Design” certification.

To learn more about how you can secure your network from evolving threats, visit telus.com/**cybersecurity**

TELUS Business