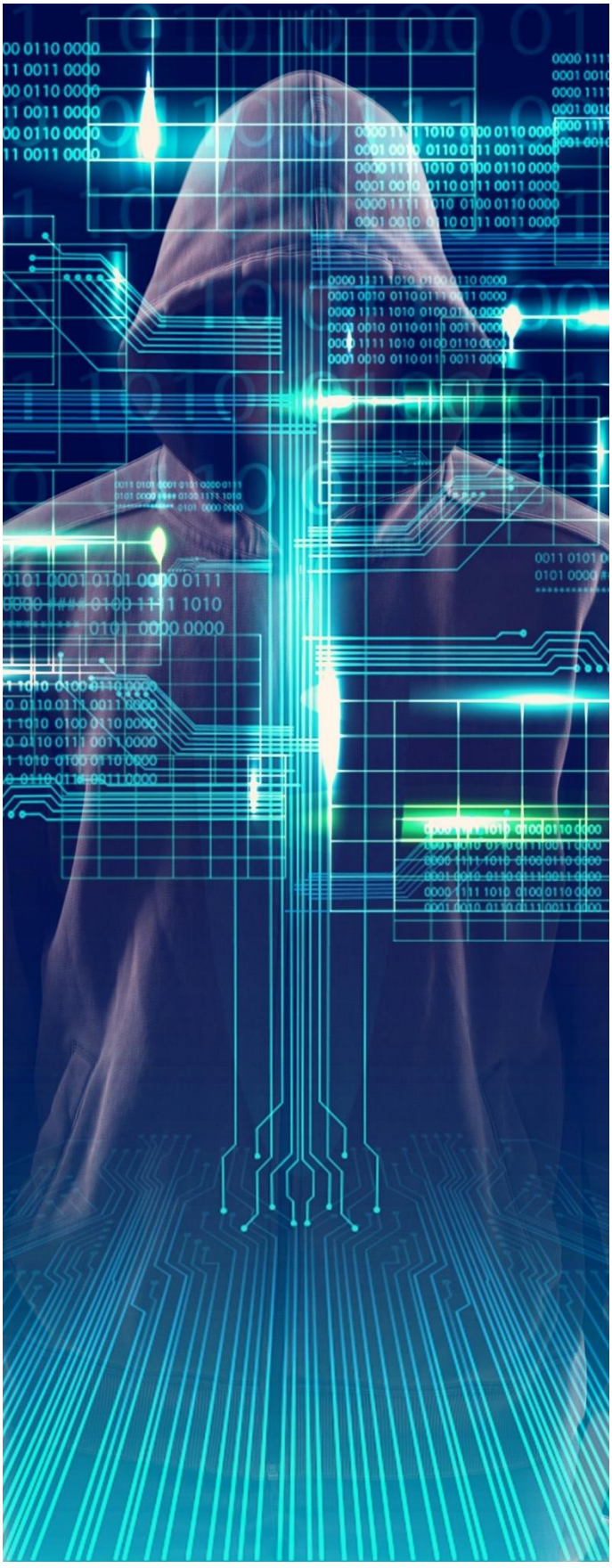
RANSOMWARE:
IMPACT & INSURANCE PERSPECTIVE



WHAT IS RANSOMWARE?

A ransomware is a type of malware (software designed to perform malicious actions) that blocks access to the victim's data, typically by encrypting files, until a ransom is paid to the attacker. The main perpetrators of ransomware attacks are known as cyber criminals, individuals or groups of individuals who carry out computer attacks for financial gain.

These attacks have become a critical threat to organizations worldwide, with cybercriminals increasingly targeting sectors that hold large amounts of Personally Identifiable Information (PII), Protected Health Information (PHI) and PCI Data (Payment Card Industry) such as healthcare, education, and government.

In 2024 and into 2025, ransomware activity in Canada has remained severe, with LockBit, BlackCat (ALPHV), Black Basta, Play, CLOP, Akira, and 8Base among the most active groups targeting Canadian organizations. According to the *Canadian Centre for Cyber Security's 2025–2026 National Cyber Threat Assessment*.

The increasing sophistication and volume of these attacks have highlighted the growing threat of ransomware, making them one of the most disruptive forms of cybercrime affecting Canadian organizations this year.

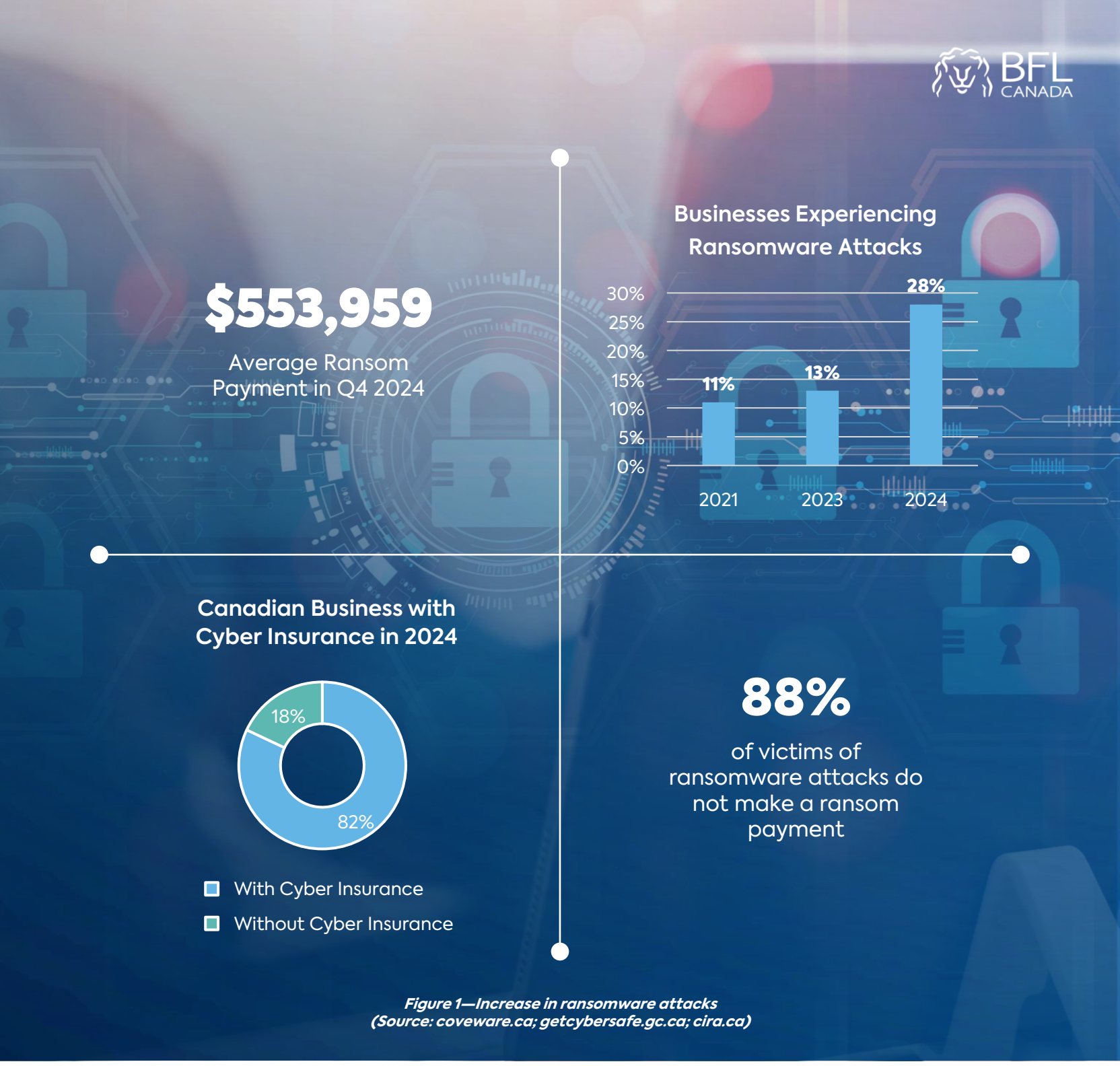


Figure 1—Increase in ransomware attacks (Source: coveware.ca; getcybersafe.gc.ca; cira.ca)

We can build a kill-chain-based model (a model used to identify and describe the stages of a cyberattack) for a ransomware attack. The most important part is how the attacker gains initial access to the company's network through social engineering by sending malicious emails, phone calls, etc. Then the attacker finds a way to elevate his privileges to achieve his goal and encrypt all the data on the system, and then they demand a ransom.

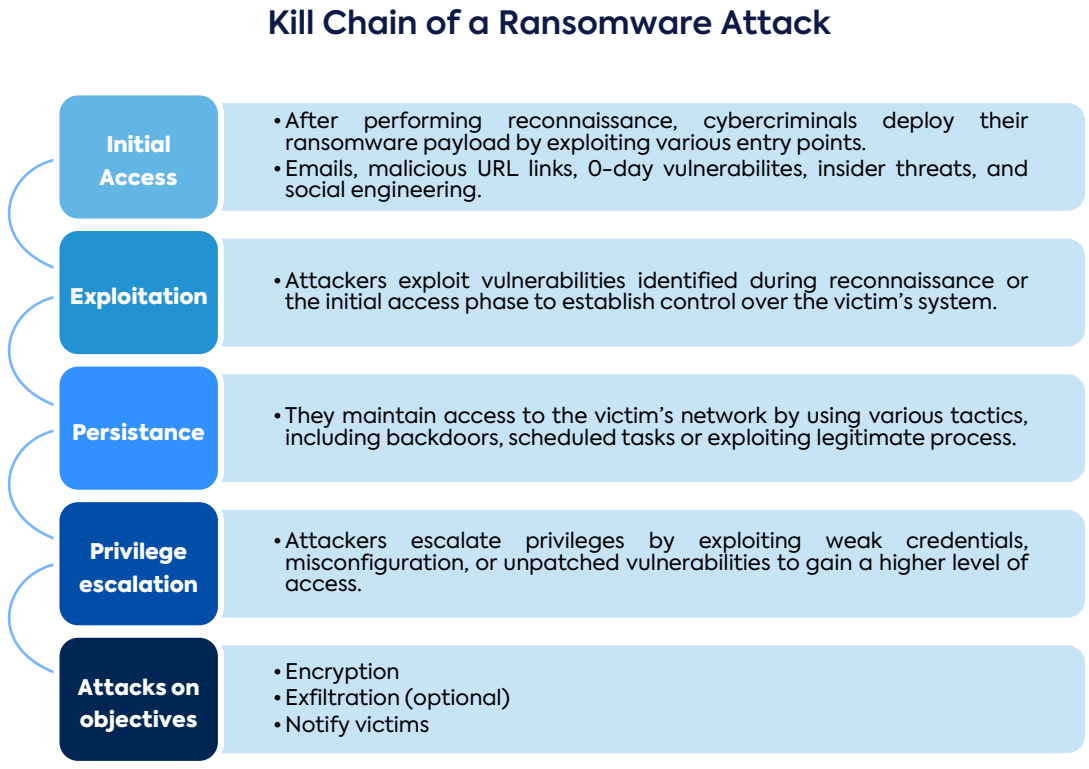


Figure 2—Example of a kill chain that attackers could use in a ransomware attack

TYPES OF RANSOMWARE EXTORTION

As the effectiveness of traditional ransomware attacks, where criminals primarily relied on data encryption to extort victims (simple extortion), decreased, double extortion ransomware emerged as a response. Simply locking data became less effective due to improved backup solutions, recovery processes, and cyber insurance adopted and purchased by organizations. By adding the threat of exfiltration of sensitive data, attackers created the strongest incentive for victims to pay the ransom.

In 2019, the criminal group known as TA2102 carried out the first high-profile double extortion ransomware attack by using Maze ransomware to breach the Allied Universal security staffing firm. This evolution not only amplified the financial pressure on organizations but also introduced a layer of reputational risk, as the potential exposure of confidential information could lead to severe consequences. Double extortion has become a prevalent strategy in the ransomware landscape, highlighting the need for organizations to enhance their security protocols and data protection measures.

Beyond simply encrypting files, this type of cyberattack may involve additional strategies such as distributed denial-of-service (DDoS) attacks, which consist of

sending large volume of data to prevent a service from being available. This strategy is considered triple extortion. The DDoS works because the ransom is not paid. Quadruple extortion involves threatening third parties with ransom demands. The figure below shows the four phases of ransomware extortion. Cybercriminals create multi-extortion ransomware to force victims to pay the ransom. In the next part of the article, we will see if it is recommended or not to pay the ransom.

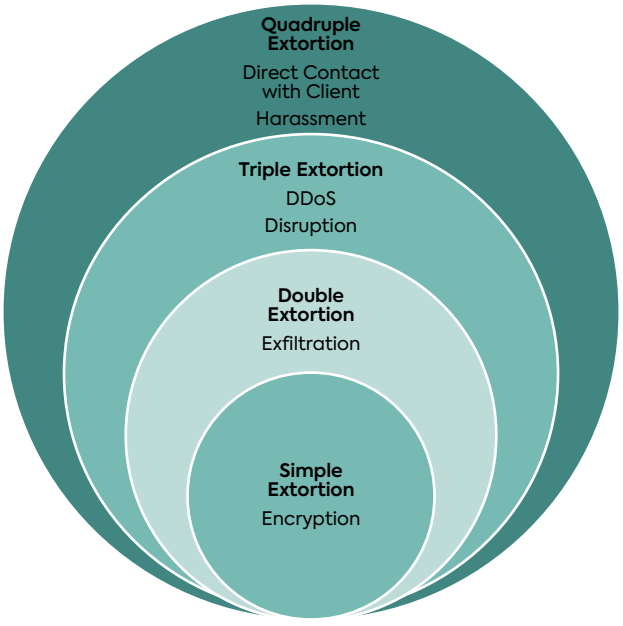


Figure 3—Four phases of ransomware extortion

RANSOMWARE NEGOTIATIONS & POTENTIAL RANSOM PAYMENT

Deciding whether to pay the ransom or not is a complex and challenging dilemma for victims. While paying may seem like a quick way to regain access to encrypted data and minimize operational disruptions, it does not guarantee that the attackers will provide the decryption key or that the data will be restored without issues. Moreover, paying the ransom can encourage further attacks, as it signals that the organization is willing to comply with demands. Victims must weigh the potential consequences of payment against the possibility of recovering data through backups or alternative recovery methods. That is why the targeted company should get help from a breach coach (hired by a ransomware negotiation company) or directly ask the insurer. The main goal of the negotiation is to gain time to assess the extent of the damage and determine if it is possible to recover the data without paying the ransom. This time can also be used to deal with the insurer or broker to manage the incident on the insurance side.

During a ransom negotiation, the negotiator will ask the attackers questions to assess the likelihood of getting the data back, or, in contrast, if the attackers are not reliable.

A sample of these questions may include:

- Is the group already known for ransomware attacks and, if yes, are they reliable?
- Can they extend the payment deadline?
- What will happen if we refuse to pay?
- What guarantees can they provide that the decryption will work?

These questions can be grouped into four categories: Threat Intelligence, Negotiation, Risk Assessment, and Assurance & Verification. A non-exhaustive timeline (*Appendix*) lists these questions with description and classification.

According to Coveware, a ransomware responder company, the average number of companies paying the ransom has decreased over the last few years. **We have observed a 60% decrease in ransom payments between 2019 and 2024.** There are several reasons why insurers often ask companies not to pay ransoms.

1. Data Backup.
2. Cybercriminals cannot be trusted to fulfill their promises. There is also no guarantee that they will decrypt data after a ransom is paid.
3. Data has already been compromised and is likely to be released, reinforcing the point that paying a ransom is unnecessary or does not prevent attackers from publishing this sensitive data.

RANSOMWARE & INSURANCE

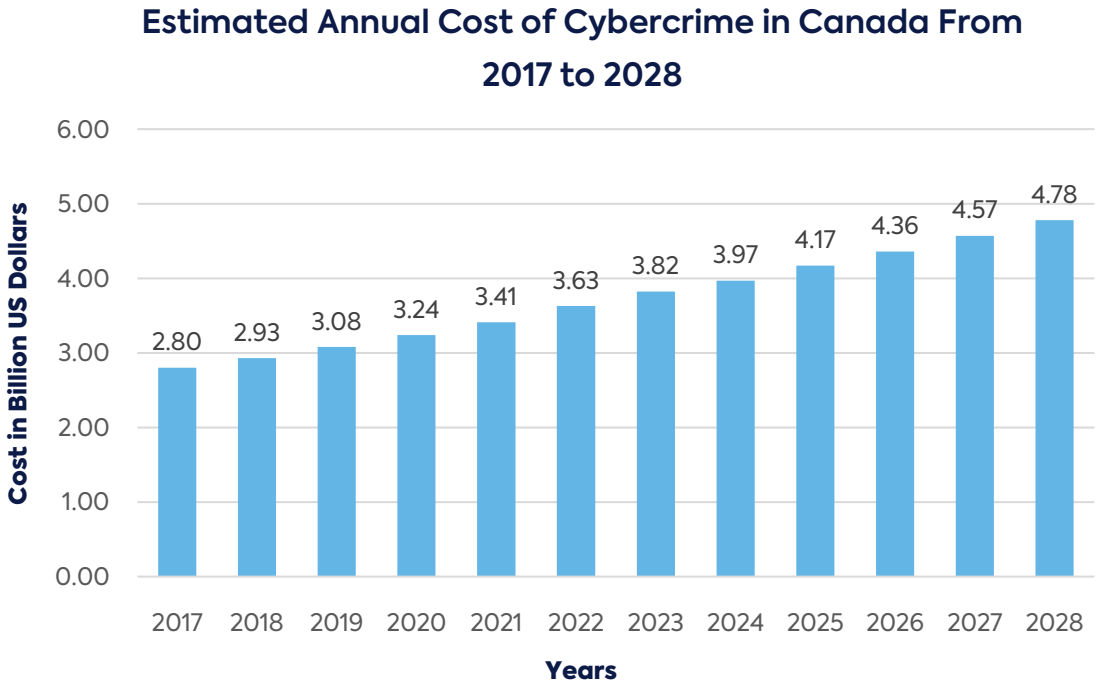


Figure 4—Estimated cost of cybercrime in Canada from 2017 to 2028 (Source: Statista)

As shown in Figure 4 above, data from Statista indicates that the cost of cybercrime is expected to rise. A significant portion of this threat comes from ransomware attacks. Given the growing risk posed by ransomware, it is critical to understand how a robust cyber policy can help mitigate the financial impact of such incidents.

RANSOMWARE EVENTS COVERED BY CYBER POLICY

A cyber insurance protects against most of the events that can be caused by a ransomware attack, providing financial support and resources for recovery. Below is a table highlighting the key ransomware events typically covered by cyber insurance policies, demonstrating the breadth of protection available to organizations facing these evolving cyber threats. **An important highlight for ransom payment, if the organization wants to pay the ransom, it must communicate with a written notice to the insurer.**

Ransomware Event	Description
Data Encryption	Coverage for financial losses incurred when critical data is encrypted and held for ransom by attackers, including costs associated with data recovery.
Data Exfiltration	Protection against costs arising from theft of sensitive information, including potential legal fees and client notifications.
Business Interruption	Coverage for lost income and extra expenses resulting from operational downtime due to a ransomware attack, helping organizations manage the financial impact.
DDoS Attacks	Financial support for mitigating distributed denial-of-service (DDoS) attacks that may accompany ransomware events, disrupting services and operations.
Legal and Regulatory Costs	Coverage for legal expenses related to data breaches, including compliance with data protection regulations and potential fines.
Public Relations and Crisis Management	Support for communication strategies and reputational recovery efforts following a ransomware incident, essential for maintaining stakeholder trust.
Forensic Investigation	A forensic investigation following a ransomware attack is critical to validating insurance claims. It helps identify vulnerabilities and informs risk management strategies to prevent future incidents.

To ensure adequate protection against ransomware attacks, clients must thoroughly understand the terms and conditions of their cyber insurance policies. This includes carefully reviewing the coverage limits, exclusions, and special conditions that may apply to various ransomware events. It is important to clarify what types of incidents are covered, such as data encryption, exfiltration, or business interruption, and to be aware of any deductibles or waiting periods that may affect claims. In addition, clients should inquire about the claims process and post-incident support services available to them. By gaining a clear understanding of their policy, clients can make informed decisions and effectively prepare their organizations for potential cyber threats.

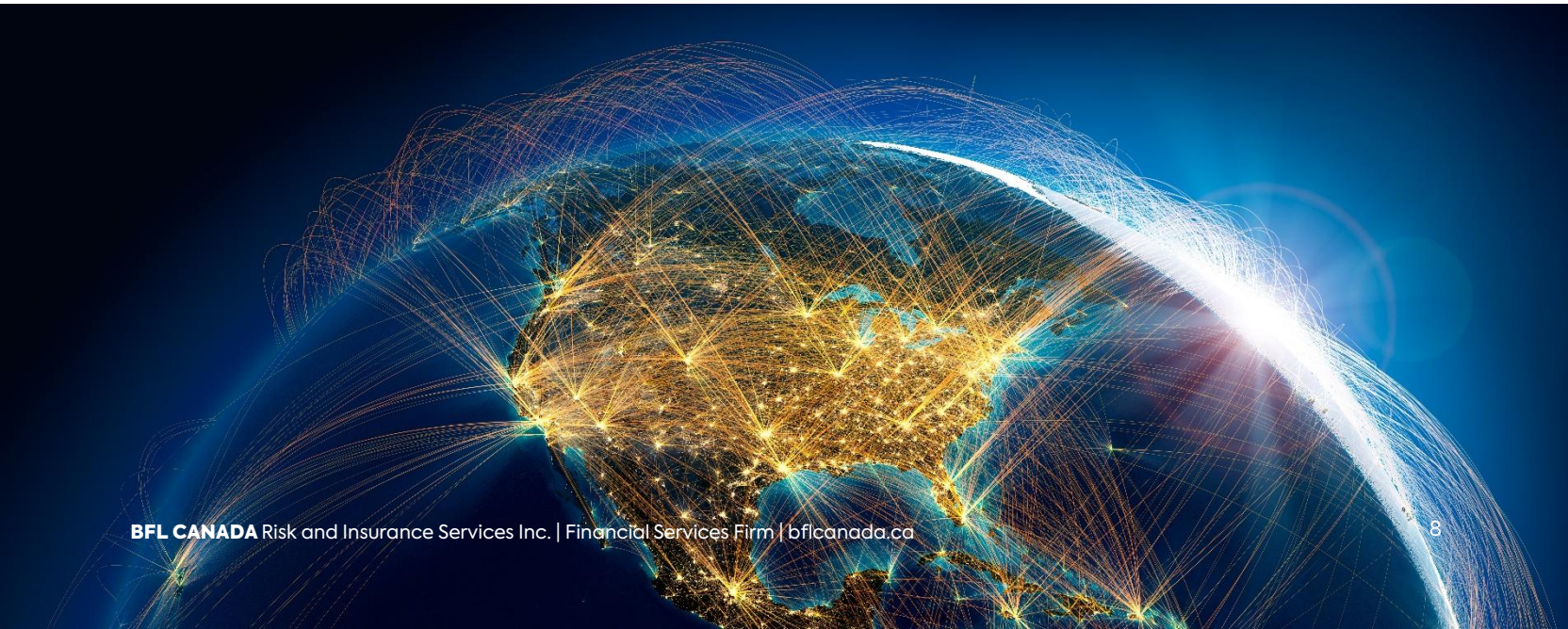
In addition to the ransom itself, organizations face significant financial impact, including business downtime that can result in lost revenue and recovery costs to restore data and systems. Legal fees may be incurred if client data is compromised, as well as potential regulatory fines for inadequate data protection.

Cyber insurance plays an important role in helping organizations recover by providing access to expert teams to assess and respond to incidents, while encouraging better cybersecurity practices and risk management. Insurers can incentivize investment in cyber hygiene, helping to reduce vulnerability to attack, although the impact on cybercriminal behaviour must also be considered.

CYBER INSURANCE AS SOLUTION

Ransomware attacks are a major concern in cyber risk discussions, as they are increasing in frequency and severity and represent a significant portion of cyber losses. While ransom payments attract attention, overall losses from ransomware go beyond extortion demands.

BFL CANADA can put you in touch with the right people to help you deal with a cyber incident or prevent such attacks, by offering you the opportunity to speak with a breach coach, conduct a forensic analysis, or address any issues related to your insurance policy.



THIS DOCUMENT WAS ISSUED BY:

BFL CANADA—Risk Advisory Services & Cyber Practice
2001 McGill College Avenue, Suite 2200
Montreal (Quebec) H1A 1G1

cyberpractice@bflcanada.ca

T. 514-843-3632
F. 514-843-3842

Toll free: 1-800-465-2842

Threat Intel

Negotiation

Risk Assessment

Assurance & verification

Is the group already known for ransomware attacks and, if yes, are they reliable?

Cybercriminal groups need to have a "good" reputation with their victim in order for them to make the ransom payment. If the group is untrustworthy, the victim has no interest in paying the ransom.

What is the ransom amount?

Knowing the ransom amount can help you make an immediate decision. The insurance limit gives the amount the insurer is prepared to pay in the event of a cyber attack. If the ransom is too high in relation to the limit, it may be better not to pay. If the amount is very low compared with the statistics, the group of attackers may not be reliable.

What forms of payment do they accept?

Ransomware attackers typically demand payment in cryptocurrencies due to their anonymity. Understanding accepted payment methods will help in discussions with cybersecurity experts and insurance providers to explore all available options and implications.

What will happen if we refuse to pay?

This step mainly saves time. In most cases, if the victim refuses to pay, they will not have access to the decryption key. In addition, it can provide information on the attackers' intentions as to whether they wish to further compromise the company.

What will they provide in return for the payment?

When a ransomware payment is made, attackers typically promise to provide a decryption key or tool that will restore access to the encrypted data. This key is supposed to unlock the files and allow the victim to regain control of their systems and data. However, It's important to note that there are no guarantees that the attackers will deliver on their promises, hence the next question.

What guarantees can they provide that the decryption will work?

Attackers often provide limited guarantees that decryption will work after the ransom is paid with a small sample decryption to prove that they could decrypt the files. In addition to this aspect, the reliability of the cybercriminal group comes into play in determining whether the decryption will work historically.

Can they verify the encryption status of our files?

This question refers directly to the previous one. To prove that the group is indeed the author of the encryption, a portion of the key used to decrypt some files can be used to verify the group's authenticity.

How can we be sure of our security if we do pay?

Paying the ransom can give the victim a reputation that encourages cybercriminal groups to target the victim again. What's more, ransomware extortion makes it even more complicated to know whether data security is guaranteed.

Can they extend the payment deadline?

Ransomware attackers often set strict deadlines to pressure victims into paying quickly. However, it is possible to negotiate an extension, sometimes for an additional fee. This can provide more time to gather funds or explore other solutions. It's crucial to approach these negotiations carefully and consult with breach coaches and experts for the best outcome.

Appendix—Timeline for Ransomware Negotiation