Ransomware playbook

ITSM.00.099

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Overview

Ransomware is a type of malware that denies a user's access to a system or data until they pay a sum of money. It can have a devastating impact on organizations and individuals. Vital data and devices can be rendered inaccessible, leaving organizations unable to conduct business or serve clients.

We have seen an increased number of ransomware attacks affecting Canadian organizations and individuals. The Cyber Centre's National Cyber Threat Assessment 2025-2026 (NCTA) specifically notes that ransomware is the top cybercrime threat facing Canada's critical infrastructure. Ransomware directly disrupts critical infrastructure entities' ability to deliver critical services, which can put the physical and emotional wellbeing of victims in jeopardy. In the next 2 years, threat actors carrying out ransomware attacks will remain a significant threat to Canada.

Threat actors have adjusted their tactics to include coercing victim organizations to pay a ransom by threatening to release stolen data or authentication credentials to publicly embarrass the organization. The NCTA notes that threat actors will very likely continue leveraging advancements in areas like artificial intelligence (AI) and cryptocurrency while developing new extortion tactics to increase their financial reward. Ransomware incidents have become more sophisticated, targeted and complex. It is increasingly difficult for organizations to defend against and recover from these attacks, especially if an organization has limited cyber security resources.

Threat actors have also become more covert in their operations. They start by gaining access to an organization's communications systems to identify critical systems and high-value data that could cause reputational damage if leaked to the public. Threat actors then deploy the ransomware to the datasets and systems of highest importance or value, compromising the organization. In addition, threat actors actively monitor the organization's communications and planned recovery actions to undermine response efforts and further infiltrate networks and connected devices.

The information provided in this publication is intended to inform organizations and help them reduce the risks of ransomware attacks, lessen the impact of these attacks, and take preventative actions. It can also help organizations to articulate business and security requirements and implement relevant policies and procedures related to cybercrime.

This publication introduces ransomware, threat actor motivations and gains, and measures to prevent these attacks and protect your organization. This publication is broken down into 3 sections:

- **Ransomware explained:** In this section, we define ransomware and outline the common vectors used to infect networks and devices

- **How to defend against cyber threats:** In this section, we provide a list of preventative measures you can take to protect your organization and offer checklists for specific mitigation measures. When you apply these measures, you enhance your cyber hygiene and protection against cyber incidents and threat actors, including ransomware.
- **How to recover from ransomware incidents:** This section includes guidance on immediate actions organizations can take when ransomware is discovered, recovery measures, and methods to evaluate the incident and enhance security measures. By following the recommendations in this section, organizations can better respond to an incident and decrease the risk of your organization being a repeat victim of ransomware.

If you believe you are a victim of ransomware:

1. Read the advice and guidance on how to recover in How to defend against cyber threats
2. Report the ransomware incident:
    a. to your local police
    b. to the Canadian Anti-Fraud Centre
    c. to the Cyber Centre
3. Once your recovery efforts are in place, read How to recover from ransomware incidents for advice on how to improve your cyber security environment

Table of Contents

List of figures

Ransomware explained

Ransomware is a type of malware that denies a user's access to files or systems until a sum of money is paid. Ransomware has evolved to also include incidents where data theft and extortion is used in place of encryption. Ransomware incidents can devastate your organization by disrupting your business processes and critical functions that depend on network and system connectivity. For more information on the evolving ransomware threat in Canada, read Ransomware threat outlook 2025-2027.

How ransomware works

When ransomware infects a device, it either locks the system or encrypts the storage, preventing access to the information and systems on your devices. Threat actors can also use your compromised network to spread the ransomware to other connected systems and devices.

The following actions can lead to ransomware infecting your networks and devices:

- visiting unsafe, suspicious, or compromised websites
- opening attachments or files from familiar or unfamiliar sources that have been infected
- clicking on links in emails, social media and peer-to-peer networks
- inserting an infected peripheral device (for example, a USB flash drive) into a different device
- exposing your systems to the Internet unnecessarily or without robust security and maintenance measures, such as
    - not implementing intrusion detection and prevention systems (IDPS)
    - operating end-of-life or unpatched devices
    - not using multi-factor authentication (MFA)

If your organization falls victim to ransomware, users or administrators will receive a notification indicating that files have been encrypted and will be inaccessible until the ransom is paid. You may also receive a message on your lock screen indicating that your device is locked and inaccessible until the ransom is paid. The message will instruct you to pay a ransom to unlock the device and retrieve the files.

Cybercriminals often request payment in the form of cryptocurrency because it can be difficult to trace the transfer. The Financial Transactions and Reports Analysis Centre of Canada stated in 2023 that the most prevalent form of money laundering involving virtual currencies is the movement of

proceeds derived from fraud and ransomware attacks. You could also be asked to pay with prepaid credit cards or gift cards. Threat actors will give you a time limit to pay the ransom, after which they may increase the ransom amount, destroy your files permanently or leak your data. More sophisticated tactics may include double extortion. A threat actor not only encrypts a victim's data but also steals it before encryption. This means the victim faces 2 threats: having to pay to decrypt their data and pay again to prevent public release of the stolen data.

The National Cyber Threat Assessment (NCTA) 2025-2026 states that threat actors are constantly evolving their strategies and adapting their techniques to maximize profits and evade law enforcement detection. These financial incentives combined with the flexibility of the ransomware-as-a-service (RaaS) model have almost certainly bolstered threat actors' resiliency in the face of law enforcement disruptions.

Ransomware attacks have become more sophisticated and often employ a combination of attack vectors. These may include sending a phishing email to your organization or conducting attacks on authentication, which is when the threat actor uses login attempts or password guessing to access your systems.

Ransomware can also spread to the systems and networks of other organizations connected by supply chains. For example, an organization that provides services to clients via interconnected networks and client management systems could be targeted by ransomware. The threat actor could then use the interconnected networks or client management systems to infect other organizations within the supply chain with ransomware. These organizations would then be locked out of their systems, disrupting their operations.

The new generation of artificial intelligence (AI), agentic AI, introduces a transformative risk to cyber security by enabling ransomware operations that are:

- **autonomous**: AI agents are no longer reliant on human intervention and can act independently throughout the attack lifecycle
- **efficient**: activities like reconnaissance, exploitation, encryption, which once took days or weeks, can now be compressed into minutes
- **adaptive**: these agents can assess their environment, select optimal tactics, evade detection and recover from failed attempts dynamically
- **covert**: AI with capabilities to erase traces and obfuscate behaviour make forensic investigations much more difficult

In practice, agentic AI can discover weak points in a network, bypass defences, deploy malware and erase evidence of the intrusion, all in a single AI-managed activity stream. However, just as agentic AI poses a new challenge for cyber security, it also offers potential defensive benefits. Security teams could deploy autonomous AI agents to monitor networks, detect anomalies or even create decoy systems that mislead attackers. They can detect early indicators of intrusion, such as sudden file encryption, unauthorized access attempts, or abnormal lateral movement within systems. Unlike traditional monitoring tools, agentic AI doesn't rely solely on known signatures; it uses behavioural analysis and anomaly detection to identify novel or stealthy threats that might otherwise go unnoticed.

When a ransomware threat is detected, agentic AI can autonomously initiate a rapid incident response. This may include isolating infected endpoints from the network, terminating malicious processes, restoring files from secure backups and notifying human security teams. These actions, which typically take minutes or hours when performed manually, can be executed in seconds, significantly reducing the impact of an attack.

It is crucial to carefully assess the risks and establish appropriate oversight when integrating AI into an organization's ransomware detection and mitigation chain. Consider the following safeguards:

- Data categorization: Categorize data at every stage (training, validation, inference and monitoring) to evaluate risk factors related to privacy, security, robustness and ethical considerations.
- Beyond standard software assurance: Assess input data quality, model use cases, and system dependencies. Map AI-vetting procedures to the Cyber Centre's IT security risk management: A lifecycle approach (ITSG-33) security controls, tailored to your organization's risk profile.
- Continuous monitoring: Employ automated tools for anomaly detection, output drift and system telemetry. Closely monitor for unauthorized model updates or unexpected behavioural changes. Robust auditing, logging and incident response mechanisms must be established for accountability and forensic analysis.
- Guardrails and controls: Implement technical guardrails for data inputs/outputs, application programming interfaces (APIs) and, where applicable, enforce Model-Context-Protocol (MCP) standards. Guardrails should account for the model's multilingual functionalities and prevent misuse in both human and computer languages.
- Human-in-the-loop oversight: Ensure critical response decisions involve qualified personnel to minimize risks associated with false positives/negatives, hallucinations or adversarial

manipulation of the large language models. Prevent high-impact automated decisions without human review.

- Periodic retraining: For locally managed models, perform routine retraining using validated, diverse, and unbiased datasets to maintain resilience and reduce systemic risks.
- Governance and accountability: Develop and maintain organizational policies, roles, and accountability structures focused on overseeing risk management across the AI lifecycle, in accordance with the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (RMF) and Cyber Centre guidance. If deployed as part of the Government of Canada (GC), ensure that the Treasury Board of Canada Secretariat (TBS) Directive on Automated Decision-Making is adhered to.

Agentic AI represents a major shift in the cyber security landscape, offering both enhanced offensive capabilities for attackers and powerful new defensive tools for organizations.

Figure 1 below provides a visual representation of how ransomware can infect an organization's networks and devices. It highlights the 3 main access vectors commonly used in ransomware incidents:

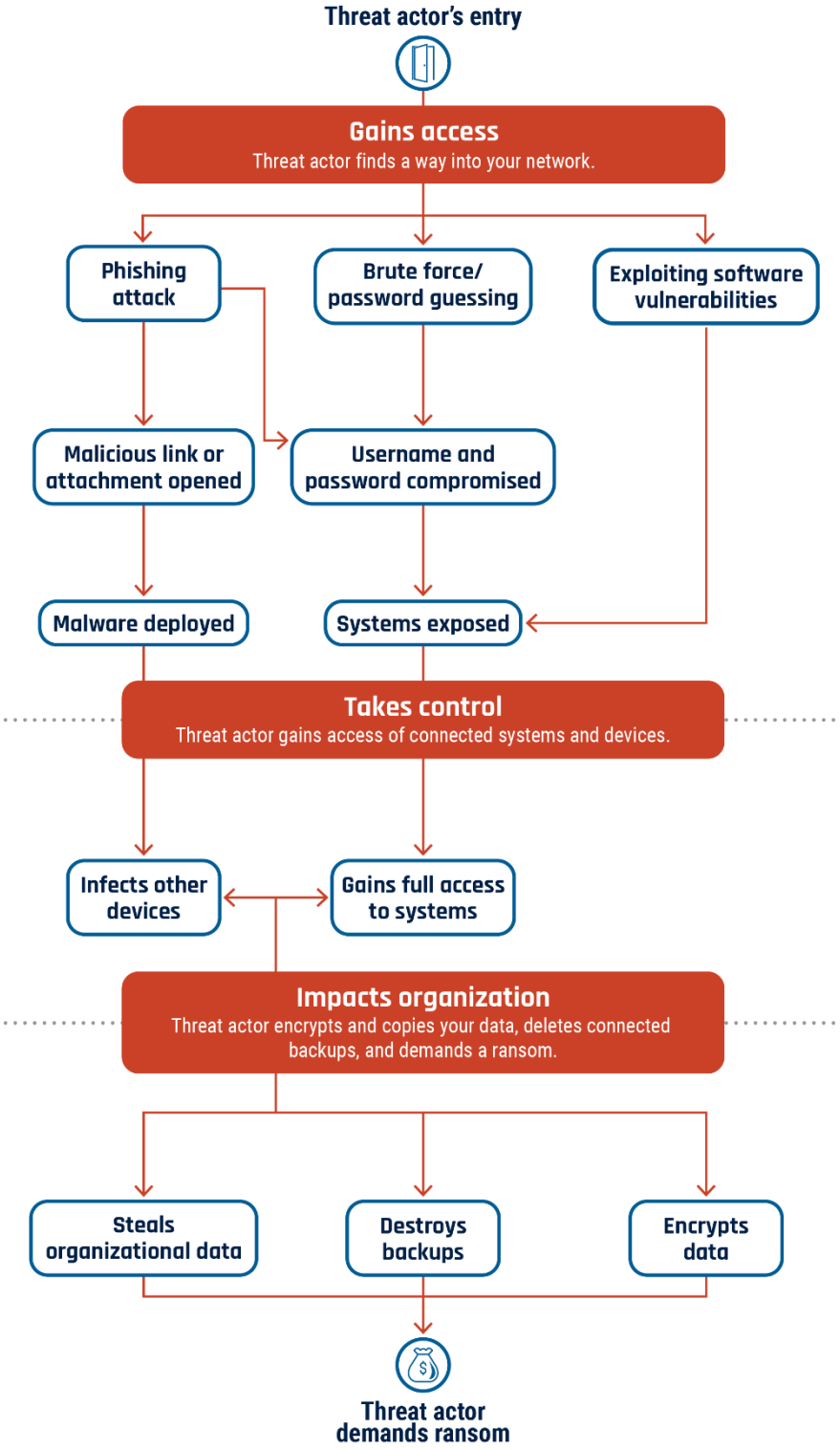
- attacks on authentication (password guessing)
- exploiting vulnerabilities in your software
- executing phishing attacks

Figure 1 also highlights the 3 stages of a ransomware incident:

1. The threat actor gains access to your network
2. They take control of your systems and connected devices
3. They deploy the malware payload to infect your systems and connected devices with ransomware

Once the threat actor has full control of your network, systems and devices, they can encrypt your data, delete available connected backup files and often steal your organization's data. They may threaten to leak this data if you do not pay the ransom, or they may say they will decrypt your data and restore your access to it if you pay the ransom.

Figure 1: How ransomware incidents occur



Long description – Figure 1: How ransomware incidents occur

This image depicts the methodology that a threat actor generally uses to gain access to your network, systems and connected devices. There are 3 stages to a ransomware incident. The threat actor:

- gains entry to your network, systems or devices
- takes control and deploys the ransomware
- encrypts your data, destroys your backups and steals your organizational data then demands a ransom payment to have your access restored

During the first phase of the ransomware incident, a threat actor usually finds their entry point to your network through:

- brute force (password guessing)
- vulnerabilities in your software
- phishing attacks
    - the threat actor attempts to solicit confidential information from an individual, group or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain
    - phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information, which they may then use to commit fraudulent acts

Once the threat actor has gained access to your network, they move onto the second phase of the ransomware attack: taking control of your systems and connected devices. They deploy the malware payload and infect your systems and connected devices with ransomware.

Once they have full control, the threat actor will move onto the third phase of the ransomware attack by encrypting your data, deleting available or connected backup files and often stealing your organization's data. They may threaten to leak this data if you do not pay the ransom, or they may say they will decrypt your data and restore your access to it if you pay the ransom.

Common ransomware vectors

Threat actors can exploit many vulnerabilities and leverage many attack vectors to infect your network, systems, and devices with ransomware. The following are examples of the most common ransomware vectors used by threat actors.

Cybercrime-as-a-service

With cybercrime-as-a-service (CaaS), specialized threat actors sell stolen and leaked data and ready-to-use malicious tools to other cybercriminals online, enabling their illicit activities. The CaaS ecosystem is underpinned by flourishing online marketplaces.

Ransomware-as-a-service

RaaS is a CaaS business model in which threat actors, regardless of their skills, can purchase malware from developers on the dark web. The developers receive a portion of the ransom paid by the victim. Most of the top ransomware groups affecting Canada operate on a RaaS business model where a core group of ransomware actors sell or lease their ransomware variant to affiliates who launch attacks. The NCTA 2025-2026 judges that the continued popularity of RaaS is almost certainly contributing to the rise in ransomware incidents by lowering the technical and administrative barriers to entry for more actors to carry out attacks.

Phishing

Phishing is a type of social engineering attack that uses text, email or social media to trick users into clicking a malicious link or attachment, revealing sensitive information or making a change in a system. Phishing attempts are often generic mass messages and can appear to be legitimate and from a trusted source, such as a bank. For more information on phishing, read Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101).

Drive-by download

Drive-by download occurs when a user unknowingly visits an infected website and unintentionally downloads and installs malware onto their device or system.

Malvertising

Malvertising injects malicious code into legitimate online advertisements. When a user clicks the ad, malware spreads to their device. Some malvertising does not even rely on user interactions and can distribute malicious code simply by being displayed.

Exposed services

Exposed services, such as Remote Desktop Protocol (RDP) and content management systems, allow access to your systems. Threat actors can use a variety of tactics, such as exploiting common vulnerabilities and password spraying, to access your devices via these exposed systems and deploy ransomware.

Email spoofing

Threat actors can use managed service provider (MSP) identities and other third-party identities to spoof emails or conduct phishing attacks against your organization. To better protect your organization from these types of threats, read our publication Cyber security considerations for consumers of managed services (ITSM.50.030).

Supply chain attacks

Supply chain attacks allow threat actors to infiltrate a service supply organization and force an update to connected customers, which can then infect their systems and devices with ransomware. The Cyber Centre provides guidance on how to secure your organization's supply chain in our publication Cyber supply chain security for small and medium-sized organizations (ITSAP.00.070).

Ransomware targets

In the NCTA 2025-2026, the Cyber Centre assessed that ransomware directed against Canada will almost certainly continue to target large enterprises and critical infrastructure providers. This, however, does not mean that other organizations or individuals are safe from the threat of ransomware. Any organization can be the victim of ransomware given the need for data to carry out core business functions. The NCTA states that in the next 2 years, ransomware actors will almost certainly escalate their extortion tactics and refine their capabilities to increase pressure on victims to pay ransoms and evade law enforcement detection.

As with most cybercrimes, ransomware attacks are financially motivated. Threat actors will target organizations of any size and demand a ransom amount based on what they believe an organization will pay to recover its encrypted data.

Ransomware attacks can have major impacts, including:

- privacy and data breaches
- reputational damage
- productivity loss
- legal repercussions
- recovery costs
- damage to infrastructure and operations

Ransomware actors are mostly opportunistic and do not necessarily target specific industries. However, ransomware is the top cybercrime threat facing Canada's critical infrastructure because it can immobilize critical business operations, destroy or damage important business data and reveal sensitive information. In addition to the financial losses associated with repairing and restoring systems and operations, ransomware attacks can disrupt critical services and jeopardize the safety and wellbeing of victims and those that rely on their services.

Critical infrastructure is an attractive target for ransomware actors because they perceive these entities as more willing to pay large ransoms to prevent disruptions to critical operations. According to the NCTA, ransomware victims in 2023 were becoming less likely to pay ransom demands. The perceived opportunities to earn high profits, combined with victims' reduced willingness to pay, has almost certainly encouraged more technically sophisticated ransomware groups to elevate their extortion techniques and hire skilled affiliates capable of targeting critical infrastructure entities to extract larger ransom payouts.

Small and medium-sized organizations are also targets, as threat actors consider their security measures to be weaker and more susceptible to attacks. Small and medium-sized Canadian organizations that are victims of ransomware will likely continue to give into ransom demands rather than face losing business or having to rebuild their networks. They likely also fear the potentially destructive consequences of refusing payment.

Cyber threat actors often steal information during a ransomware attack. Threat actors can hold data for ransom, sell it or use it to gain an unfair competitive advantage by exploiting proprietary or patented information. The theft of organizational information, including intellectual property and

customer and client data, can have both short- and long-term financial consequences for victims. These include impacts to global competitiveness, reputational damage and identity theft.

Vendor concentration is increasing organizations' vulnerability to cyber threats like ransomware. A small number of large digital service providers, each with a large user base, provide many technology services. A cyber incident involving a single, dominant service provider can therefore affect an entire sector. Cyber threat actors target dominant vendors to steal customer data or demand ransom payments. The compromise of dominant service providers can amplify the impact of cyber security incidents. Cyber threat activity against services that are digital chokepoints (single points of failure within supply chains) can cause cascading and system-wide disruptions to the economy and society and endanger national security.

Finally, the cyber threat surface is expanding. In addition to the ongoing adoption and deployment of the Internet of Things (for example, connected vehicles), the boom in AI platforms and services is forecasted to drive demand for supporting infrastructure and lead to the transfer of even more data to cloud environments. It is also likely that AI-focused organizations are now more prominent targets for cyber threat actors and ransomware.

Ransomware payment

The decision to pay a cybercriminal to release your files is difficult, and you will likely feel pressured to give into their demands. Before you even consider paying, contact your local police department to report the cybercrime. Paying the ransom will not guarantee access to your encrypted data or systems.

The decision to pay the ransom is up to your organization, but it is important to be fully aware of the risks associated with paying. For example, threat actors may use wiper malware, which alters or permanently deletes your files once you pay the ransom. Paying the ransom also validates RaaS as a business model, which will encourage its growth and fund new attacks. Payment may also be used to fund other illicit activities, possibly including organized crime, terrorism or state-sponsored violence. Furthermore, it may be unlawful to pay ransom under laws against terrorism, money laundering, funding criminal organization activities, or sanctions legislation. Even if you pay, threat actors may still:

- demand more money
- continue to infect your devices and systems or those of other organizations
- retarget your organization with a new attack

- copy, leak or sell your data

The NCTA 2025-2026 displays the relative number of Canadian ransomware incidents reported to the Cyber Centre by Canadian victims between 2021 and 2024. Based on our data, the number of ransomware incidents has increased, on average, by 26% each year. Since many ransomware incidents go unreported, it is almost certain that the true number of ransomware incidents impacting Canada is higher than what is displayed. The Canadian Survey of Cyber Security and Cybercrime (CSCSC), conducted by Statistics Canada on behalf of Public Safety Canada, reported that the total recovery costs associated with cyber security incidents in 2023 doubled to $1.2 billion CAD.

How to defend against cyber threats

Ransomware is among the most common types of malware and can be one of the most damaging cyber attacks to your organization. Single mitigation measures are not robust enough to combat the evolving threat of ransomware. Your organization should adopt a defence-in-depth (multi-layer) strategy to protect its devices, systems, and networks from ransomware and other types of malware and cyber attacks. Your strategy should include multiple layers of defence with several mitigation measures or security controls at each layer.

Cyber defence planning

There are many approaches you can take to better protect your networks, systems, and devices. The following is a list of security controls you can implement to strengthen your cyber security posture.

Develop your backup plan

Develop and implement a backup plan for your organization. A backup is a copy of your data and systems that can be restored in the event of an incident. There are several types of backups you can implement to protect your organization's information:

- **Full:** You may want to do a full backup periodically (weekly or monthly) and before major system upgrades. A full backup is the most expensive and time-consuming option, depending on the amount of information being backed up and your storage requirements.
- **Differential:** A differential backup only creates a copy of data that has changed since your last full backup.
- **Incremental:** With incremental backups, you are only storing the data that has changed since your last full or differential backup. Each increment is saved as an incremental volume. If you need to restore data, you must process each increment, which can be time consuming.

Storing your backups

There are 3 options for storing your backups: online, offline, and in the cloud.

Online backups are:

- stored within the physical space of your organization
- readily available should you need to initiate your recovery process
- susceptible to data loss in the event of a natural disaster or power surge

- vulnerable to ransomware if connected to your systems or networks

Offline backups (also known as cold backups) are:

- stored in separate physical locations from your organization's main centre
- disconnected from your networks

Although data loss and theft are still possible, but having backups offline can prevent threat actors from accessing and infecting your backups with ransomware.

Cloud backups are:

- stored on a cloud platform, often maintained by a cloud service provider (CSP)
- available through your CSP's server and can be accessed from anywhere
- encrypted in the cloud for additional security, but data loss and cyber attacks (including ransomware) can still occur

Protecting your backups

Many ransomware variants are designed to locate, spread to and delete your system backups. Threat actors see this action as additional assurance to receive payment from your organization. If the ransomware spreads to your backups, you will be unable to restore and recover your systems and data, which ultimately halts your business operations. Most commonly, backups stored online or in the cloud are susceptible to ransomware. Storing your organization's backups offline offers you the most protection against ransomware incidents.

Your organization should implement an offline backup process. Your backups will not be connected to your networks or devices, which ensures ransomware cannot locate and delete your backups. Ensure your organization has multiple backups stored offline and conducts the backup process frequently, to guarantee data is as close to real time as possible. Testing your backups is also a crucial element to your backup and recovery process. To ensure an additional layer of protection, you should encrypt your backups. The Cyber Centre's Guidance on becoming cryptographically agile (ITSAP.40.018) and the Cyber Security Readiness Goals Cross-Sector Toolkit provide information on strong and agile encryption for data in transit.

Having a secondary backup in the cloud is also a recommended approach to enhancing your ability to recover. These backups will ideally be managed by a CSP within their secure cloud infrastructure. CSPs will provide an additional layer of security for your organization. Note that your organization is always legally responsible for protecting its data. You should ensure that the service provider you

select can support your security, backup and recovery requirements with proper safeguards. You should also consider data residency, which refers to the geographical location where your data is stored. Your organization may have regulatory and policy requirements to ensure data is stored in Canada. If you plan to contract a vendor for offsite storage, make sure that they have security measures, incident management processes and a disaster recovery plan in place.

Note: Your CSP can also be a victim of ransomware, which can indirectly impact your organization. You may not be able to access the data you have stored in the cloud, which can significantly impact your ability to do business. You may also face issues with data integrity and confidentiality.

Recommendation: The recommended approach to backing up your information is to have multiple backups in multiple locations. You should have 2 or more backups stored offline and inaccessible by your networks and internet connection. You could then have a secondary backup in the cloud with your CSP. You should implement a schedule to test your backups on a regular basis (for example, monthly). Having 1 or more backup files available provides your organization with an increased chance of recovering and getting back to business more quickly if you are the victim of ransomware, or any other cyber incident.

For more information on developing your backup plan, see Tips for backing up your information (ITSAP.40.002).

Develop your cyber incident response plan

Developing an incident response plan for your organization is the keystone to your cyber defence strategy. You should also consider developing a disaster recovery plan for your organization. In these 2 plans, your organization considers major events that could cause an unplanned outage and could require you to activate your recovery response. Your incident response plan helps you detect and respond to cyber security incidents. Your disaster recovery plan focuses on how the organization recovers and resumes critical business functions after an incident.

There are many benefits to developing an incident response plan:

- Effective incident management lessens the impact of a cyber incident
- A practiced plan will help you make good decisions when under the pressure of managing a real incident
- Key actions are approved in advance, allowing financial authorities and resources to be available in the immediate steps of your incident response

- A well-managed response, with clear communication throughout, builds trust with stakeholders and customers
- Learning from incidents identifies gaps in and issues with your response capability

Your incident response plan should cover several key elements. The main goal is to recover from an incident as quickly as possible. The following checklist provides an overview of the key elements you should include in your incident response plan. It is not a comprehensive list of incident response requirements, but it does provide a structured approach and action items that your organization can implement.

By following this checklist in the preliminary stages of your incident response plan, you can identify your risks, devise a plan of action to mitigate them and prepare your organization for an efficient recovery that will allow you to get back to business quickly.

For more information on developing your incident response plan, read Developing your incident response plan (ITSAP.40.003).

Cyber incident response plan checklist

Use the following incident response plan checklist to ensure your incident response is complete.

- Conduct a risk assessment:
  - identify key systems and assets that are critical to your business operations
  - analyze the likelihood and impact of these systems being compromised
  - prioritize your response efforts to ensure the most critical systems and assets are protected and backed up offline frequently and securely
- Develop policies and procedures:
  - develop an incident response policy that establishes the authorities, roles and responsibilities for your organization
  - establish and communicate pre-authorizations to contract assistance to key incident response contacts
- Establish your cyber incident response team (CIRT):
  - create a CIRT to
    - assess, document, and respond to incidents
    - restore your systems, recover information

        - reduce the risk of another ransomware incident occurring
    - include employees with various qualifications and have cross-functional support from other business lines
    - designate backup responders to act for any absent CIRT members in the event of an incident
- Deliver training:
    - tailor your training programs to your organization's business needs and requirements and to your employees' roles and responsibilities
    - ensure your training includes the cyber security controls listed (for example, spotting malicious emails and phishing attacks and using strong passphrases)
    - for advice and guidance on cyber security event management training, email the Cyber Centre Learning Hub at education@cyber.gc.ca. The Learning Hub offers a comprehensive event management course that can be tailored to your organization's business and information technology (IT) needs
- Identify stakeholders:
    - identify the internal and external key stakeholders who will be notified during an incident. You may have to alert third parties, such as clients and MSPs
    - depending on the incident, you may need to contact law enforcement and possibly a lawyer
- Develop a communications plan:
    - detail how, when and with whom your team communicates
    - include a central point of contact for employees to report suspected or known incidents
    - ensure you have external contact information for all members and backup members of your CIRT, key personnel and key stakeholders
    - prepare sample media statements that can be tailored to cyber incidents as they occur
    - consider retaining a third-party ransomware recovery organization that can guide you through your incident response and recovery process

Incident response process

Your incident response process will follow a 4-phase lifecycle.

Phase 1: Prepare

- Assign policies
- Define goals
- Test backup processes
- Test patch and update processes
- Track vulnerabilities
- Develop test exercises

Phase 2: Observe

- Develop a monitoring strategy (for example, frequency, included networks)
- Monitor your networks and connected devices for threats
- Generate event and incident reports regularly
- Analyze the data and determine whether you need to activate your response

Phase 3: Resolve

- Analyze your findings to fully understand the incident
- Determine which mitigation measures need to be put in place (for example, disconnect devices)
- Run antimalware and antivirus software
- Patch vulnerabilities
- Restore your systems and data via your backup
- Preserve evidence and document steps taken

Phase 4: Understand

- Identify the root cause of the incident
- Evaluate your incident response and highlight areas requiring improvement

- Meet with your response team and develop lessons learned and future initiatives to improve your response

Use these 4 phases to structure your plan and your response. A primary part of your incident response should include reporting cybercrimes :

- to your local police department
- online to the Canadian Anti-Fraud Centre
- online to the Cyber Centre

Develop your recovery plan

Your recovery plan should complement your backup plan and incident response plans. When developing your recovery response, consider many variables and clearly identify and document what is to be recovered, by whom, when and where.

Guidelines for your recovery plan

Use the following guidelines for your recovery plan.

Planning

- Identify stakeholders, including clients, vendors, business owners, systems owners and managers
- Identify your response team members and their roles and responsibilities
- Take inventory of your hardware and software assets
- Identify and prioritize critical business functions, applications and data
- Prepare emergency documentation—such as a contact list for all employees, clients, service providers and suppliers—to ensure you can react quickly and efficiently in the event of a ransomware incident
- Conduct a tabletop exercise to ensure all participants are aware of their roles and required actions in the event of a ransomware attack
- Invest in cyber security insurance if you determine it to be beneficial for your organization. This may add an additional layer of protection and may also provide your organization with incident response expertise in the event of a ransomware attack

Measuring

- Set clear recovery objectives
- Define data backup and recovery strategies
- Test your plan

Communicating

- Develop a communications plan to inform key stakeholders
- Develop a training program for employees to ensure everyone is aware of their roles, responsibilities and the order of operations during an incident
- Connect with your MSPs to identify areas where they can assist you with your recovery efforts
- Engage IT security specialists prior to an event to ensure you have subject-matter experts weighing in on your response and recovery efforts

To create an effective plan, you should identify your organization's critical data, applications and functions. Critical data may include financial records, proprietary assets and personal information. Critical applications are the systems running key functions that are imperative to your business. You will need to restore critical data, applications and functions immediately to ensure business continuity in the event of an unplanned outage or incident. You should consider conducting a risk assessment to help identify critical business functions and the relevant threat and vulnerability risks.

To ensure your response is effective, your organization should run through specific scenarios such as a cyber attack, a significant power outage or a natural disaster. This will help you identify key participants and stakeholders, address significant risks, develop mitigation strategies and determine recovery time and effort.

You can conduct a business impact analysis (BIA) to predict how disruptions or incidents will harm your operations, business processes, systems and finances. Almost all recovery processes will require a significant period without Internet connectivity to evict the attackers. Plan for this downtime in your BIA.

In your BIA, you should also assess the data you collect and the applications you use to determine their criticality and choose priorities for immediate recovery. It is also critical to take note of your recovery efforts, documenting what went well and what areas require improvement.

To learn more about developing your recovery plan, read Developing your IT recovery plan (ITSAP.40.004).

Manage user and administrator accounts

Oversee the creation and assignment of user and administrator accounts with secure access in mind. Consider creating separate accounts for non-administrative functions (for example, access to email and limited access to internal systems) to reduce the risk of ransomware infecting your administrator accounts and the system access associated with those accounts. You should limit administrator accounts to those who need full or specialized access to your organization's network, systems and devices. Ensure you have complete segregation of duties for backup administrators relative to primary/production administrators. Pay particular attention to possible common or federated authorization management systems, such as directory services or cloud identity providers.

Your organization should use dedicated administrative workstations (DAWs) to create secure environments exclusively for privileged operations. Removing public Internet access from administrative workstations can substantially reduces risk of compromise. Remote access to privileged accounts should be performed on DAWs governed entirely by the system's security policies and used exclusively for this purpose.

If a threat actor gains access to an administrative account, they can use the elevated privileges to affect your organization's operating environment, attack your network or access sensitive information. Attackers can also learn what detection and recovery activities exist on your systems, which may help them avoid discovery and prevent you from stopping further attacks.

To manage access to your systems and data, apply the principle of least privilege. That is, only provide employees with access to the functions and privileges necessary to complete their tasks. You should also use the principle of least privilege when allowing remote access to your devices. Ensure you activate MFA at all access points into your network. Consider using single sign-on (SSO) access where possible to enhance the security of your devices and connected networks. Restrict administrative privileges and require confirmation for any actions that need elevated access rights and permissions.

When assigning administrator accounts or privileged access to users, your organization should take the following measures:

- use strong authentication methods for your accounts
    - use MFA for all administrative accounts
    - use a unique passphrase for each privileged account
    - change default passwords to unique passphrases for applications and devices
    - authenticate users before they are granted access to applications or devices

- ensure that unique, identifiable accounts are attributed to individual users
- log and monitor actions on privileged accounts
- provide training on expected behaviours for privileged account users
- remove special access privileges when users no longer require them
- decommission and delete user accounts when someone leaves the organization

To address the modern challenges of securing remote workers, protecting hybrid cloud environments and defending against cyber security threats, we recommend you implement a zero trust (ZT) security model. ZT's central tenet is that no subject (application, user or device) in an information system is trusted by default. Trust must be reassessed and verified every time a subject requests access to a new resource. The degree of access provided is dynamically adjusted based on the level of trust established with the subject. ZT involves adopting a new mindset to security by always assuming a breach and focusing on protecting resources (for example, services and data). For more information about ZT security models, read A zero trust approach to security architecture (ITSM.10.008). In addition to managing your accounts, it is also imperative to manage the decommissioning and disconnecting of obsolete or retired systems and devices. These systems and devices must be removed from your network, sanitized and disposed of securely.

For more information on managing access and administrative accounts, read:

- Top 10 IT security actions - Managing and controlling administrative privileges (ITSM.10.094)
- Best practices for passwords and passphrases (ITSAP.30.032)

Cyber security controls

When implementing and maintaining a defence-in-depth model, your organization must layer security controls throughout your networks to protect the security, confidentiality, integrity and availability of your networks, devices and information.

As shown in Figure 2 below, a variety of security controls, layered throughout your networks, can better defend your organization from ransomware. Some of the cyber security controls identified in Figure 2 can be applied at various stages or in various areas within your network and systems. For example, logging, alerting and network segmentation should be applied in all layers of your defence-in-depth strategy.

To proactively mitigate threats during the first stage of a ransomware incident, it is essential to have key preventative measures and cyber security controls in place before an incident occurs. By

implementing the following controls as part of your security environment, you can strengthen your organization's ability to detect, contain, and minimize the impact of ransomware threats early on.

- Provide your employees with tailored cyber security training to ensure they are aware of attack vectors like phishing and know how to identify suspicious emails or links
- Use strong passphrases to deter authentication attacks
- Implement MFA for your organization's devices and systems
- Create an application allow list to control who or what is allowed access to your networks and systems. Application allow lists help to prevent malicious applications from being downloaded and infecting your server
- Scan your hardware, software and operating system for vulnerabilities. Apply patches and updates to mitigate the risk of the vulnerabilities being exploited by a threat actor
- Segment your network to ensure sensitive and high-value information is in a separate zone of your network
- Set up monitoring and logging functionality for your systems and networks and ensure you receive automated alerts if any anomalies are detected
- Protect systems that are connected or exposed to the Internet with
    - encryption
    - firewalls
    - IDPS
    - frequent vulnerability assessments
- Deactivate macros to decrease the risk of ransomware being spread through attachments and ensure that users cannot reactivate them
- Block advertising to prevent ads, especially malvertising, from being displayed

To help mitigate the threats that take place during the second stage of a ransomware incident, you can implement the following measures to better protect your systems and networks and prevent ransomware from spreading across your network and connected devices:

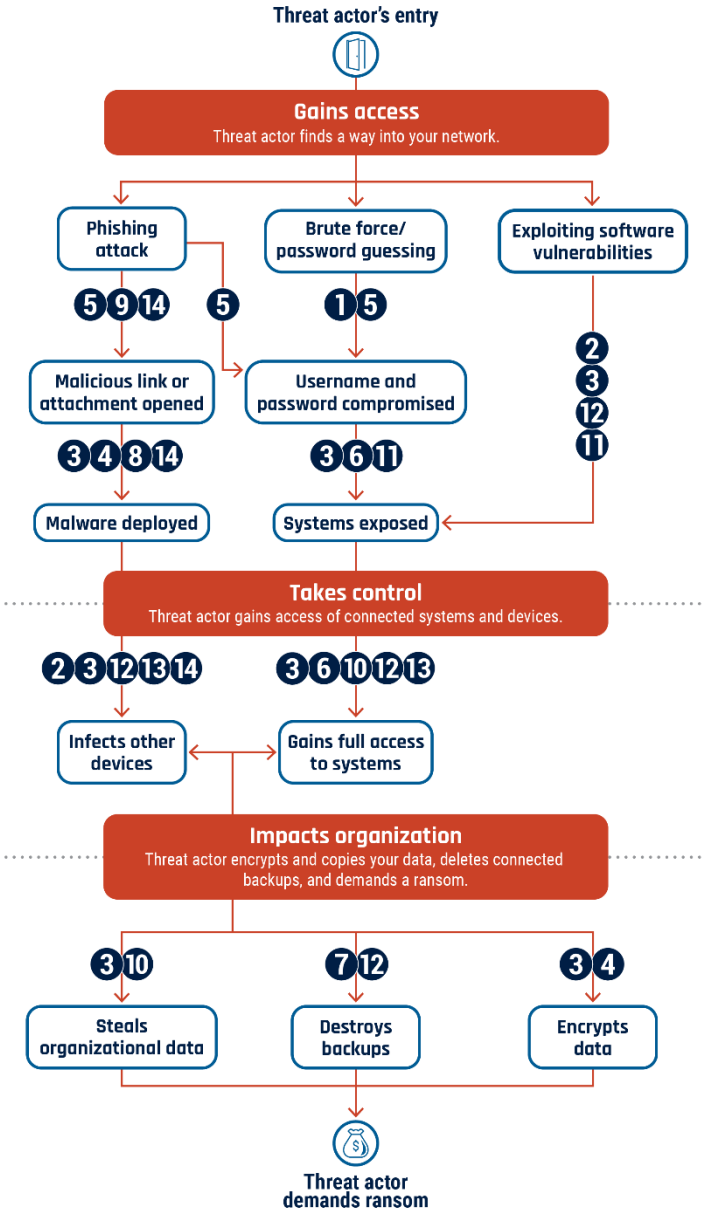
- Use security tools, such as antivirus and antimalware software
- Use firewalls and IDPS on your networks to help protect potential entry points against threat actors
- Apply the principle of least privilege

In the third stage of a ransomware incident, the top pre-emptive mitigation measure for your organization is its backup plan. Ensure you have multiple copies of your backups stored offline. By having your backups disconnected from all networks, network-based threat actors will be less likely able to delete them or infect them with ransomware. Ensure that you test your backups and restore processes on a regular basis. Address any issues immediately to ensure your backup files are ready for your organization to recover quickly in the event of a ransomware incident.

The following section provides more detailed guidance on the various security controls your organization can implement. For more information on security controls, read:

- Baseline cyber security controls for small and medium organizations
- Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)

Figure 2: Security controls to reduce the risk of a ransomware incident



Long description – Figure 2: Security controls to reduce the risk of a ransomware incident

Figure 2 shows the same methodology that a threat actor uses to conduct a ransomware attack but highlights where security controls can be implemented to mitigate and attempt to prevent the ransomware attack from occurring.

In the first stage of a ransomware incident, under the “gains access” section of this diagram, there are some preventative mitigation measures that can be put in place to protect your organization. The following is a list of cyber security controls that can be implemented at the forefront of your cyber security environment:

- Provide your employees with tailored cyber security training to ensure they are aware of attack vectors like phishing and how to identify suspicious emails or links
- Use of strong passwords, or preferably passphrases, to attempt to prevent threat actors from being successful in brute force attacks
- Implement MFA for your organization’s devices
- Create an application allow list to control who or what is allowed access to your networks and systems. Application allow lists help to prevent malicious applications from being downloaded and infecting your server
- Scan your hardware, software and operating system for vulnerabilities. Apply patches and updates to mitigate the risk of the vulnerabilities being exploited by a threat actor
- Segment your network to ensure sensitive and high-value information is in a different zone of your network
- Setup monitoring and logging functionality for your systems and networks and ensure you receive automated alerts if any anomalies are detected
- Protect your systems that are connected or exposed to the Internet with
    - encryption
    - firewalls
    - MFA
    - frequent vulnerability assessments
- Disable macros to decrease the risk of ransomware being spread through Microsoft Office attachments

In the second stage of a ransomware incident, under the "takes control" section of this diagram, there are some mitigation measures you can implement to enhance the protection of your systems and networks and to prevent ransomware from spreading across your network and connected devices:

- Implement security tools, such as antivirus and antimalware software and firewalls, to your networks to add layers of protection to potential entry points for threat actors
- Apply the principle of least privilege in which you provide individuals only the set of access privileges that are essential for them to perform authorized tasks

In the third stage of a ransomware incident, under "threat actor impacts organization," the number 1 mitigation measure you can implement for your organization is your backup plan. Ensure you have multiple copies of your backups stored offline and, if possible, in the cloud through a CSP. By having your backups disconnected from your network, threat actors cannot delete them or infect them with ransomware. Ensure you test your backup and restore processes frequently and adjust any issues immediately to ensure your backup files are ready for your organization to recover quickly in the event of a ransomware incident.

Create an application allow list

An application allow list is a corporate portfolio of approved software. The list is enforced so that only approved software gets installed in an organization's various systems. An allow list selects and approves specific applications and application components (for example, executable programs, software libraries or configuration files) to run on organizational systems. Application allow lists help to prevent malicious applications from being downloaded and infecting your server.

Your organization can create a list of applications that are authorized for use in the workplace or that are known to be from a trustworthy vendor. When a user launches an application, it is compared against the allow list and is only permitted if it appears on the list. Hashing is used to verify the application's integrity and generates a value from a string of text that is unique to every application. If an application is updated or patched, the hash changes to ensure that you are only running the newest version of the application. A complementary measure to application allow listing is enforcing the use of approved signatures from approved software vendors for all types of software.

By implementing an application allow list, your organization will enhance your cyber defence posture and prevent incidents such as ransomware.

For more information on applications allow lists, read Implement application allow lists (ITSM.10.095).

Use protective domain name system

Domain name system (DNS) is a protocol that maps domain names that are easily read by the human eye to Internet Protocol (IP) addresses that are easily read by machines. DNS is often referred to as the address book for the Internet. DNS is used for both human-initiated actions (for example, visiting a website) and machine-initiated actions (for example, running an update).

Protective DNS is a tool that your organization can implement to block employees from visiting potentially malicious domains on the Internet when using corporate devices. Protective DNS identifies malicious domains against your organization's blocklist, which is a listing of domains and IP addresses that users are not permitted to visit using corporate assets or while on an organizational network. For more information on DNS, read Protective Domain Name System (ITSAP.40.019) and Domain Name System (DNS) tampering (ITSAP.40.021).

You should also consider implementing protective DNS filtering on any mobile devices used by your employees, especially if they can connect to your network and systems remotely. You can do this by manually configuring DNS settings on your organization's devices, through a mobile device management (MDM) tool. For more information on protecting mobile devices, read Security considerations for edge devices (ITSM.80.101).

Canadians can use a free public DNS application called Canadian Shield. The application is provided by the Canadian Internet Registration Authority (CIRA) and ensures personal devices always use a trusted DNS and filter out malicious IP addresses. Canadian Shield can be set up on your router or gateway to better protect your entire network. We recommend applying its Protected DNS resolver, which is designed to offer enhanced malware and phishing blocking. Replacing the default DNS server settings on your devices with a trusted DNS server can better protect your devices.

Establish perimeter defences

Protecting your network, connected systems and devices against cyber threats can seem daunting. Perimeter defences protect the boundary between 2 network security zones through which your traffic is routed. Defending this boundary with basic security protocols like firewalls, antivirus and antimalware software and IDPS significantly enhances your overall protection. Installing anti-phishing software is another way to strengthen your organization's cyber security. Anti-phishing software blocks phishing emails to prevent attacks from occurring or spreading further.

Ensure that users access the network using your organization's virtual private network (VPN). A VPN acts as a secure tunnel through which you can send and receive data on an existing physical network.

Using a VPN provides a secure connection between 2 points, such as your laptop and your organization's network.

Implement logging and alerting

Implementing continuous monitoring of your networks will help you establish a baseline of acceptable activity patterns within your organization. Establishing monitoring capabilities, such as intrusion detection systems (IDS) for your networks, can help your organization manage risk. Your monitoring system should generate logs that can be reviewed by IT specialists and management when necessary. You should limit access to your logs to those who need to review them.

You should also implement automatic alerting within your monitoring practices so that anomalies in activity patterns are flagged and reviewed. Automatic alerting should also identify potential vulnerabilities and events that require you to take risk mitigation action. The alerts will indicate that something out of the ordinary has occurred. Your organization can then review these anomalies to determine what occurred, whether there is a risk to the organization, and what can be done to mitigate the risk. Your organization's logging and alerting system should not permit modifications to be made to your logs once they have been received from the system. Logs should be timestamped to assist you in understanding what led to an event or an incident.

If your organization becomes the victim of ransomware or another type of cyber incident, your logs could provide insight into how the incident occurred. They could also show what controls or mitigation measures can be implemented to better protect your networks and systems from future incidents.
For more information on implementing logging and alerting, read Network security logging and monitoring (ITSAP.80.085).

Assess vulnerabilities

A vulnerability assessment can identify and prioritize known vulnerabilities that cybercriminals could exploit to gain access to applications, systems, and data. This assessment can involve:

- vulnerability scanning to identify known vulnerabilities within applications
- penetration testing, which simulates attacks that cybercriminals might perform to evaluate how well the infrastructure withstands them
- security assessments and audits to identify misconfigurations that could lead to security vulnerabilities
- intrusion detection to monitor for intrusions and intrusion attempts

- threat hunting to identify and eradicate threats using computer forensics, cyber threat intelligence and malware analysis

Segment your networks

Segmenting your network involves dividing your networks into smaller sections or zones so that traffic is directed and flows through the different sections of the network. This allows you to stop traffic flow in certain zones and prevent it from flowing to other areas in your network. In the same manner, segmentation also allows you to isolate and stop the spread of malware to different sections of your network, and to control and restrict access to your information. When segmenting your network, ensure your IT and operational technology (OT) networks are identified, separated and monitored. These networks should be air-gapped, meaning that you should physically or conceptually isolate secure computer networks from unsecure networks, such as those that connect to the Internet. In addition to segmenting your IT and OT networks, you should also identify interdependencies between them and implement measures that can be put in place during a cyber incident to protect critical information and functions.

For more information on segmenting your networks, read Segment and separate information (ITSM.10.092).

Constrain development and scripting environments and deactivate macros

If your organization uses the Microsoft Windows operating system, you may want to consider constraining your development and scripting environments. With Windows specifically, Microsoft developed an automated system administration capability through an interface powered by their shell scripting language, known as PowerShell. It is a powerful and important part of the system administration toolkit. It can be used to fully control Microsoft Windows systems and has many benefits for organizations. However, threat actors can exploit PowerShell and inject malicious code into your devices' memory. More concerning is the fact that PowerShell is a trusted source and therefore a threat actor's code injection typically will not be blocked by antivirus or antimalware software or by your systems' event logs. To make it harder for malicious PowerShell behaviour to be obfuscated, organizations should ensure that standard users are allowed to modify the relevant registry keys or the transcript folder.

Organizations should also consider using protected event logging to prevent sensitive information, such as passwords in script blocks that are logged to the event log, from being leaked.

Many organizations also have development tools, such as Python, Perl, PHP and .NET, that threat actors can exploit for malicious purposes. Isolate these tools from the user environment.

Macros are another security consideration when using Windows. Macros are written sequences that imitate user keystrokes and mouse commands to automatically repeat tasks in applications. Macros are used in many Microsoft Office products to automate processes and data flows. They are embedded in the code of the files, enabling users to create shortcuts for specific tasks (for example, sort worksheets alphabetically, unmerge all merged cells or unhide all rows and columns).

Threat actors can create malicious macros and include them in documents that they may then send to employees in your organization. To decrease the risk of ransomware being spread through Office attachments, you should set your user defaults to deactivate macros and ensure that users cannot re-activate them. You should also ensure that macros cannot contain sensitive information, such as personal credentials, and use organization-developed or signed macros that are verified by technical authorities within your organization.

For more information on macros, read How to protect your organization from malicious macros (ITSAP.00.200).

Patch and update

To protect your connected devices from ransomware, you should check the operating system, software and firmware regularly for updates and install security patches. There are a variety of patches available, but the following 3 types are most applied:

- bug fix patch: repairs functionality issues in software (for example, an error that causes unexpected device behaviour)
- security patch: addresses security vulnerabilities to protect the system from threats (for example, malware infecting devices through security flaws)
- feature patch: adds new functions to the software (for example, enhancements to application performance and speed)

For more information on patching and updating your devices, read Patch operating systems and applications (ITSM.10.096).

Manage passwords and passphrases

Your organization should implement passphrases in place of passwords where possible. Using strong passphrases is 1 step in protecting your systems and sensitive information, but it is not enough to prevent a threat actor from gaining access. Password guessing is a common tactic used by threat actors to gain access to networks and systems. If using passphrases is not possible, you should use strong, unique passwords combined with MFA.

Subsection 'Manage user and administrator accounts' provides details on adopting MFA in your account and access management practices. In combination with using MFA, you should encourage employees to use a password manager. Password managers can be beneficial for remembering and securing passwords or passphrases required to access your networks and systems.

Your organization should also consider implementing password vaults for administrative accounts. Password vaults ensure a higher level of protection since the passwords or passphrases are cycled and synchronized with your systems. This ensures a password or passphrase can only be used once. It also provides tracing capabilities that can determine who used a password or passphrase at a given time for specific access.

For more information on the implementation and use of password managers, read Password managers: Security tips (ITSAP.30.025) and Best practices for passphrases and passwords (ITSAP.30.032).

Protect email domains

Threat actors may leverage misconfigurations or gaps in cyber security protocols to advance their goals. They often target email systems with the aim of gaining unauthorized access, stealing sensitive information or disrupting communication channels. Email accounts house a large amount of private information, including personal data, financial details and confidential business exchanges. Ensuring secure email communications is important to prevent breaches that could compromise the integrity of these exchanges. Email security also protects against malware and phishing attacks, which are frequently initiated via deceptive emails.

Consider implementing technical security measures to protect your organization's domains from email spoofing, prevent the delivery of malicious messages sent fraudulently on behalf of your domain and identify the infrastructure used by threat actors. These measures also help prevent phishing emails from being delivered to your organization. You can reduce a threat actor's chance of carrying out successful malicious email campaigns by implementing the following 3 security

protocols that act jointly to protect email domains from being spoofed. For more information, read Quick guide to email configuration (ITSAP.60.003).

Sender Policy Framework

Sender Policy Framework (SPF) is a system that uses features of DNS and allows domain owners to specify which servers are authorized to send emails on behalf of their domain. If you receive an email from an IP address that is not specifically permitted by the SPF record, it is likely not legitimate. When an email is sent, the recipient's mail server checks the SPF record of the sender's domain to see if the sending mail server is on the authorized list. If the sending mail server is included in the SPF record (a "pass"), the email is considered legitimate and is usually delivered. However, if the sending mail server is not listed in the SPF record (a "fail"), the recipient's mail server may handle the email cautiously, possibly rejecting it or marking it as spam.

DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) is an email authentication protocol that enhances the security of email messages by allowing the sender to digitally sign them. When an email system that supports DKIM receives a DKIM-signed message, it retrieves the record associated with the message's DKIM header and verifies the message's signature using the published public key. This DKIM check cryptographically confirms that the message was sent by an authorized sender and was not altered in transit. If the signature is not valid, or if no DKIM record is available, the message will fail DKIM. Messages that fail this DKIM check may be rejected.

DKIM ensures the integrity of email communication, making sure that emails have not been tampered with. It allows recipient servers to check the message's authenticity and to confirm it originates from the claimed domain. This helps prevent spoofing and impersonation attempts.

Domain-based Messaged Authentication, Reporting and Conformance

Domain-based Messaged Authentication, Reporting and Conformance (DMARC) policy and verification can enhance your security protocols and protect your email domains from being spoofed. It builds on DKIM and SPF to ensure emails are authenticated before transmission, guaranteeing that they originated from the intended domain, and are sent to legitimate recipients. If an email passes through the DMARC validation, it will be delivered to the intended recipient. If the email fails DMARC validation, the receiving email system applies the policy specified in the sending domain's DMARC record and will either deliver the email, deliver the email but mark it as suspicious or reject the email.

Unlike some other solutions that rely on a single point of failure, DMARC uses a resilient strategy that covers both the source and target sides of email communication. It conducts a comprehensive security check on sender information, recipient details, subject lines, body text and other message characteristics.

For more information on email domain protection, read Implementation guidance: Email domain protection (ITSP.40.065) and Email security best practices (ITSM.60.002).

How to recover from ransomware incidents

Recovering from a ransomware incident can be a lengthy process and recovering your organization's brand and reputation can take even longer. Assuming your organization will eventually encounter some form of malware can help you develop your planned response and could speed up your recovery processing time. By adhering to the guidance provided in this document, your organization will not only reduce the time it takes to recover from an attack but can also reduce the likelihood of an attack or minimize the impact of an infection.

Recovery process

As described in subsection 'Develop your recovery plan', having reliable backups that are secured and stored offline can significantly enhance your ability to recover from a ransomware attack. If your organization has been hit with ransomware, there are immediate steps you can take to minimize the impact of the infection.

Immediate response actions

Threat actors can infiltrate your network and can gain insight into components and data in your systems, devices that are connected to your system and your communications. Once you become aware of an infiltration, you should assume that the threat actor is still on your network and is aware of what is happening in your organization. As such, you should implement an alternative communication method (for example, external email accessed by a device not connected to your network) that cannot be accessed by them. This will also block the threat actor from gaining insight into your intended incident response plans and recovery actions. Your organization can follow the checklist below when taking immediate action, ideally within the first few hours, against a ransomware attack.

Immediate response checklist: Detection, analysis, containment and eradication

Determine what is infected and isolate systems and devices

- Determine which devices and systems are infected with the ransomware
- Isolate all systems and devices
- Disconnect the infected systems and devices from the Internet and any internal network connection to reduce the risk of the infection spreading to other connected devices
- Determine what data, including data in transit, has been impacted by the ransomware

- Establish the likelihood that the confidentiality or integrity of the data has been compromised. Inform data managers and stakeholders of potential impacts
- Deactivate your VPNs, remote access servers, SSO resources and cloud-based or public-facing assets as additional measures to contain the ransomware infection

Report to law enforcement

- Report the ransomware attack to local law enforcement. Ransomware is considered a cybercrime and may be investigated by law enforcement
- Report the ransomware attack to the Canadian Anti-Fraud Centre and the Cyber Centre online via My Cyber Portal
- If you have been infected with a known type of ransomware, check if law enforcement can provide you with a decryption key

Assemble your CIRT

- Communicate the incident details to your CIRT (established while creating your incident response plan)
- Provide clear direction to CIRT members on their roles and responsibilities in managing the incident
- Document the known details to ensure your CIRT has an initial understanding of what has occurred
- Triage the systems impacted by the ransomware for restoration and recovery. This will guide your CIRT on where to focus immediate actions

Change credentials

- Reset credentials, like passwords and passphrases, for administrator and user accounts
- Ensure you are not changing any credentials that are required to restore your backup or that may lock you out of systems needed during the recovery process
- Create temporary administrator accounts to begin your recovery and monitor whether the threat actor is leveraging your original accounts

Wipe and reinstall

- Safely wipe your infected devices to remove any malware, bugs or viruses
- Reinstall the operating system to rid your devices of the infection
- Update the basic input/output system and reload firmware

Run security software

- Run antivirus and antimalware diagnostics on your backup to make sure it is clean before you begin the restore process
- Restore your systems into a clean, network-isolated location and then ensure they are at the very latest patch state for all software. This can be time consuming and may “break” system dependencies that will have to be resolved
- Scan any files that might have been accessed by the threat actor or extracted from a compromised system
- Download the Cyber Centre’s free malware detection and analysis tool Assemblyline
- Address any items flagged by the scans

Recovery actions

Although isolating your infrastructure from the Internet can temporarily disrupt your business, it is the most important course of action. Isolation will temporarily remove the threat actor’s access to your infrastructure, allowing you to gain control and further your incident investigation, response and recovery.

Once you have completed the steps identified in the checklist above and you are certain that your backups and devices are clear of any malware or viruses and are at the most recent patch state, you should begin your recovery process, as outlined in the following subsections.

Remediate the point of entry

To recover successfully and avoid reinfection, you will need to identify how the threat actor was able to enter your network, systems and devices and address the vulnerability immediately. Ensure you remediate the point of entry prior to reconnecting your systems or devices to your network or the Internet to thwart the threat actor’s ability to gain access in the same manner.

Implement your backup plan

Ensure your organization is protected by having a detailed backup plan in place. You will execute this plan if your main systems and data storage are compromised and need to be restored with your copied information. The backup plan will ensure your organization can restore critical systems and data and get back to business quickly. You should recover your systems using offsite backups that are not connected to your networks. Prior to restoring from a backup, scan and analyze it with a known uncorrupted system to ensure it has not been compromised by the threat actor.

Restore your systems

Following your incident response plan, identify the critical systems and data that need to be recovered first. Ensure that these systems and data have not been impacted by the ransomware attack and that they do not have signs of any other malware infection.

There are several options to consider when implementing your recovery strategy. You should choose a recovery strategy that meets your business needs and security requirements.

Engage cyber security professional assistance

Procuring professional services from a highly rated cyber security agency or professional can be helpful when preparing for and responding to a ransomware incident. If your organization has a cyber insurance policy, your provider will often include the assistance of a third-party cyber security professional in the event of an incident like a ransomware attack. They will provide you with incident response expertise and a recovery strategy tailored to your organization. They may also deploy an incident handling team to lead your organization's response and recovery process. If you do engage professional cyber security assistance, ensure you clearly identify the service expectations, roles and responsibilities. The introduction of cyber insurance as a proactive measure of protection against ransomware can encourage enterprises to align their cyber security postures with insurance policy standards. However, if insurance policy documents are not properly protected, sophisticated ransomware actors could obtain that sensitive information on coverage amounts and leverage it in ransom negotiations to maximize their payment from companies.

Inform stakeholders

When an incident occurs, and especially when it compromises your systems and data, it is imperative that you inform key stakeholders, clients and employees. You should consider preparing a statement in advance that can be tailored to the incident, as well as a contact list of all stakeholders to be notified. Ransomware attacks can jeopardize your organization's reputation, so your communications plan must be implemented swiftly following an incident. This will ensure your stakeholders are informed and able to enact their own incident response plans, if necessary.

Analyze the incident

It is crucial to determine the root cause of the incident. Identify how the threat actor gained access to your network and deployed the ransomware. A ransomware incident is often an indication of a more serious hack or intrusion by the threat actor. If you do not identify how a threat actor gained access or apply appropriate security measures to prevent it from happening again, threat actors may continue to exploit the vulnerability.

Note that to succeed in forensics, a high-integrity forensic record of events must be available. As for backups, monitoring and logging must have strong segregation of duties to withstand the hostile attention of attackers.

A vital step in your incident analysis is determining what systems, accounts and information the threat actor accessed. This will allow you to determine the extent of the damage, such as what accounts were compromised and what data was exfiltrated. In turn, this will inform your approach to control the attack, prepare and implement a proper response and execute a successful recovery.

Summary

Ransomware is an ever-present threat to all organizations, regardless of their size. Ransomware incidents can lead to financial loss, data breaches and reputational damage for your organization. Preparing your organization and applying proactive measures to protect your network, connected devices and information is critical for your ability to respond to and recover from ransomware.

If your organization has fallen victim to ransomware, conducting a lessons-learned exercise post-recovery is an excellent way of implementing further mitigation measures and correcting actions and strategies that did not go as planned. Revise your incident response plan based on these lessons learned to ensure your organization has the most robust response and recovery plans possible.

Consider reporting cyber incidents to law enforcement, such as local police or the Canadian Anti-Fraud Centre, and to the Cyber Centre online via My Cyber Portal. If you are comfortable doing so, share your findings, including the tools, techniques and procedures used by the threat actor, with the Cyber Centre. This will assist the Cyber Centre in providing alerts and guidance to the public and will help individuals and organizations protect their assets from the same ransomware attack. Sharing your lessons learned can benefit other organizations and the broader cyber security community.

Effective date

This publication takes effect on December 11, 2025.

This is an UNCLASSIFIED publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, contact the Cyber Centre:

- by email: contact@cyber.gc.ca
- by phone: 613-949-7048 or 1-833-CYBER-88

This version supersedes Ransomware playbook, dated November 30, 2021.

Revision history

Revision	Amendments	Date
1	First release	November 30, 2021
2	Second release	January 28, 2026