Communications
Security Establishment

Centre de la sécurité
des télécommunications

Choose a building block.

CANADIAN CENTRE FOR
CYBER SECURITY

RANSOMWARE PLAYBOOK

MANAGEMENT

Canada

FOREWORD

This document 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, email, or phone our Service Coordination Centre:

Service Coordination Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on November 30, 2021.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	November 30, 2021

D97-4/00-099-2021E-PDF
978-0-660-40617-6

OVERVIEW

Ransomware is a type of malware that denies a user's access to a system or data until a sum of money is paid. It is a serious and evolving threat to Canadians. The impact of ransomware can be devastating to organizations. Vital data and devices can be made inaccessible to organizations, leaving them unable to conduct their business or serve their clients. We have seen an increased number of ransomware attacks affecting Canadian organizations and individuals. Threat actors have adjusted their tactics to include coercing victim organizations to pay the ransom by threatening to release their stolen data or authentication credentials to publicly embarrass the organization. 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 or investment.

Threat actors have become more covert in their operations by first gaining access to an organization's infrastructure, including their communications systems, to identify critical systems, high-value data, personal information, and 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, leaving the organization compromised. In addition to this tactic, threat actors actively monitor the communications and planned recovery actions of an organization to undermine response efforts and further infiltrate networks and connected devices.

The information provided in this document is intended to inform and assist organizations with drawing down the risks, reducing impacts, and taking preventative actions associated with ransomware attacks. You can use the considerations below to articulate your business and security requirements and implement relevant policies and procedures related to cybercrime.

The document is divided into two sections:

1. How to defend against ransomware
2. How to recover from ransomware

If you have been the victim of ransomware and need advice and guidance on how to recover, see section 2 "How to Recover from Ransomware." Report the ransomware incident to law enforcement (e.g. local police and the Canadian Anti-Fraud Centre) and online via the Cyber Centre's My Cyber Portal.

Once your recovery efforts are in place, please refer to section 1 "How to Defend Against Ransomware" advice on how to improve your cyber security environment

For more information, phone or email our Services Coordination Centre:

Service Coordination Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

This document introduces ransomware, threat actor motivations and gains, and measures to prevent these attacks and protect your organization. The information presented is intended to inform you and your organization of the risks, impacts, and preventative actions associated with ransomware incidents. This document is broken down into the following two sections:

1. **Prevention:** In this section we define ransomware, outline the common vectors used to infect networks and devices, 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.
2. **Response:** This section includes guidance on immediate actions you can take when the ransomware is discovered, recovery measures that will get you back to business, and methods to evaluate the incident and enhance security measures. By following the action items in this section, you can enhance your ability to respond to an incident and decrease the risk of your organization being a repeat victim of ransomware.

1.1 WHAT IS RANSOMWARE?

Ransomware is a type of malware that denies a user's access to files or systems until a sum of money is paid. Ransomware incidents can devastate your organization by disrupting your businesses processes and critical functions reliant on network and system connectivity.

RANSOMWARE VECTORS

Phishing is an attack that uses text, email, or social media to trick users into clicking a malicious link or attachment. Phishing attempts are often generic mass messages, but the message appears to be legitimate and from a trusted source (e.g. a bank). Malicious code will execute commands using your account privileges. Threat actors may also use this opportunity to install a backdoor to your devices.

Drive-by download occurs when a user unknowingly visits an infected website where malware is downloaded and installed without the user's knowledge.

Malvertising injects malicious code into legitimate online advertisements. When a user clicks the ad, malware spreads to their device.

Exposed services, such as Remote Desktop Protocol (RDP) and content management systems, allow access to your devices. 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.

RANSOMWARE AIDS

While the following items are not traditional vectors, they are available options for threat actors to use to initiate a ransomware attack.

Third parties and managed service providers (MSP) identities can be used by threat actors to spoof emails or conduct phishing attacks against your organization. Review *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services* [1] to protect your organization.

Supply chain attacks allow threat actors to infiltrate a service supply organization and force an update to connected customers, infecting their systems and devices with ransomware. Review *ITSAP.00.070 Supply Chain Security for Small and Medium-size Organizations [2]* to secure your organization's supply chain.

Ransomware as a Service (RaaS) is a 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.

1.1.1 HOW DOES RANSOMWARE WORK?

When ransomware infects a device, it either locks the screen or encrypts the files, 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.

Your networks and devices can be infected with ransomware in the following ways:

- Visiting unsafe, suspicious, or compromised websites (known as a drive-by download);
- Opening emails or files from familiar or unfamiliar sources (phishing);
- Clicking on links in emails, social media, and peer-to-peer networks;
- Inserting an infected peripheral device (e.g. USB flash drive) into a device; or,
- Exposing your systems to the internet unnecessarily or without robust security and maintenance measures, such as patching vulnerabilities and multi-factor authentication (MFA) in place.

If your device is infected with ransomware, you will receive a notice on your screen indicating your files are encrypted and inaccessible until the ransom is paid. You may also receive a message on your lock screen indicating 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. Payment is often requested in the form of digital currency, such as bitcoin, because the transfer would be more difficult to trace. Prepaid credit cards or gift cards may also be requested. You will be provided with a time limit to pay the ransom, after which threat actors may increase the ransom amount, destroy your files permanently, or leak your data. As an additional extortion method, a threat actor may threaten to release your data publicly if you do not pay the ransom.

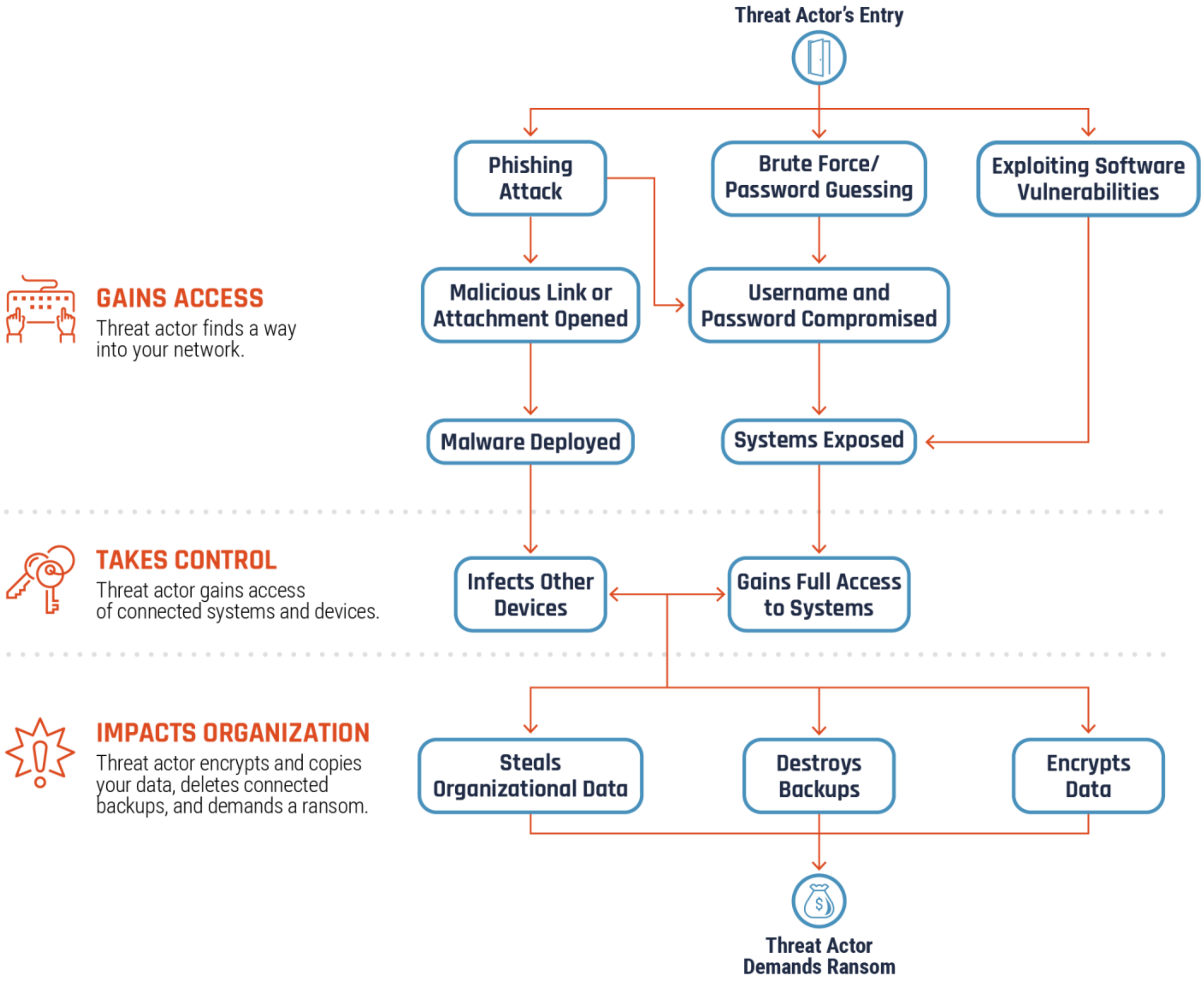
Ransomware has become more sophisticated and often employs a combination of attack vectors, such as sending a phishing email to your organization along with brute force attacks, where the threat actor uses extensive login attempts or password guessing to access your systems and networks. Ransomware can also spread to the systems and networks of organizations connected via their supply chain. For example, an organization who provides services to their clients via inter-connected networks and client management systems could be targeted by ransomware. The threat actor could then use the inter-connected 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 following diagram (Figure 1) provides a visual representation of how ransomware can infect your networks and devices, highlighting the three main access vectors commonly used in ransomware incidents: brute force (password guessing), exploiting vulnerabilities in your software, and executing phishing attacks.

Figure 1 also highlights three stages of a ransomware incident: the threat actor gains access to your network, takes control of your systems and connected devices, and then deploys the malware payload and infect your systems and connected devices with ransomware.

Once the threat actor has full control of your network, systems, and devices they will 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 [3]


Threat Actor's Entry
Phishing Attack
Brute Force/ Password Guessing
Exploiting Software Vulnerabilities
GAINS ACCESS
Threat actor finds a way into your network.
Malicious Link or Attachment Opened
Username and Password Compromised
Malware Deployed
Systems Exposed
TAKES CONTROL
Threat actor gains access of connected systems and devices.
Infects Other Devices
Gains Full Access to Systems
IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.
Steals Organizational Data
Destroys Backups
Encrypts Data
Threat Actor Demands Ransom

1.1.2 WHO DO CYBERCRIMINALS TARGET?

In our *National Cyber Security Threat Assessment 2020 (NCTA)* [4], we found that ransomware directed against Canada will almost certainly continue to target large enterprises and critical infrastructure providers. This, however, does not mean 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 conduct core business functions.

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

Ransomware attacks can have major impacts, including privacy and data breaches, reputational damage, productivity loss, legal repercussions, recovery expenses, and damage to infrastructure and operations. Organizations that cannot allow sustained disruptions are more likely to pay millions of dollars to quickly restore their operations.

Small and medium-sized organizations are also targets, as threat actors consider their security protection measures to be weaker and more susceptible to an attack. Canadian ransomware victims will likely continue to give in to ransom demands due to the severe costs of losing business and rebuilding their networks and the potentially destructive consequences of refusing payment.

Information is often stolen by cyber threat actors concurrently with the 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, including impacts to global competitiveness, reputational damage, and identity theft.

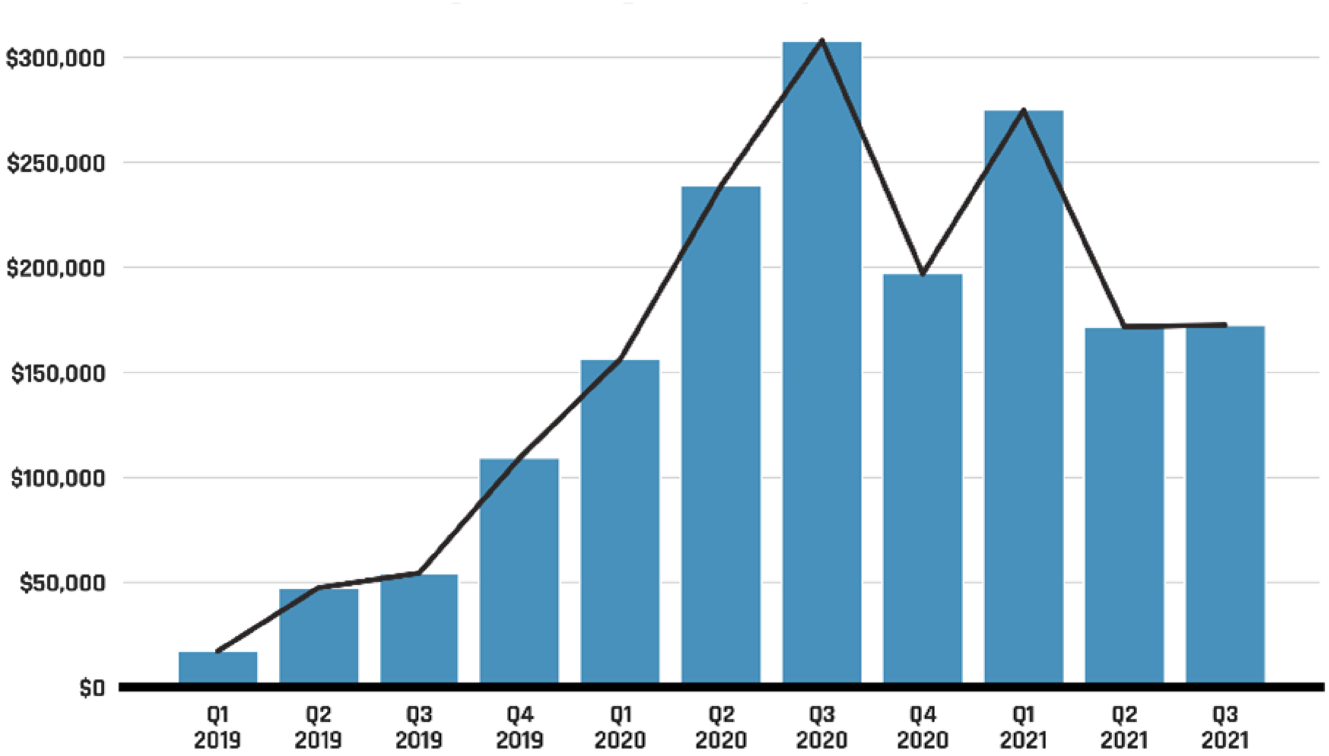
1.1.3 SHOULD YOU PAY THE RANSOM?

The decision to pay a cyber threat actor to release your files or devices is difficult, and you may feel pressured to give in to their demands. Before you pay, contact your local police department and report the cybercrime. Paying the ransom does not guarantee access to your encrypted data or systems. Ultimately, the decision to pay the ransom is your organization's to make, but it is important for your organization to be fully aware of the risks associated with paying the ransom. For example, threat actors may use wiper malware, which alters or permanently deletes your files once you pay the ransom. Payment may also be used to fund and support other illicit activities. Even if you pay, threat actors may still carry out the following actions:

- Demand more money;
- Continue to infect your devices or other organizations' devices;
- Re-target your organization with a new attack;
- Copy, leak, or sell your data.

The following chart (Figure 2) from the *NCTA 2020* demonstrates the increase in the average ransom payment over the past few years. As Figure 2 demonstrates, after increasing rapidly from 2019 to 2020, known ransom payments appear to have stabilized around $200,000 in 2021, which is down slightly from levels seen in 2020. Ransom payments are likely reaching a market equilibrium, where threat actors are becoming better at tailoring their demands to what their victims are most likely to pay given the growth of recovery cost and the risk of reputational damage from public data leaks.

Figure 2: Average Ransom Payment Over Time



2 HOW TO DEFEND AGAINST CYBER THREATS

Ransomware is one of 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 not only ransomware, but other types of malware and cyber attacks. Your strategy should include several layers of defence with several mitigation measures or security controls at each layer.

2.1 CYBER DEFENCE PLANNING

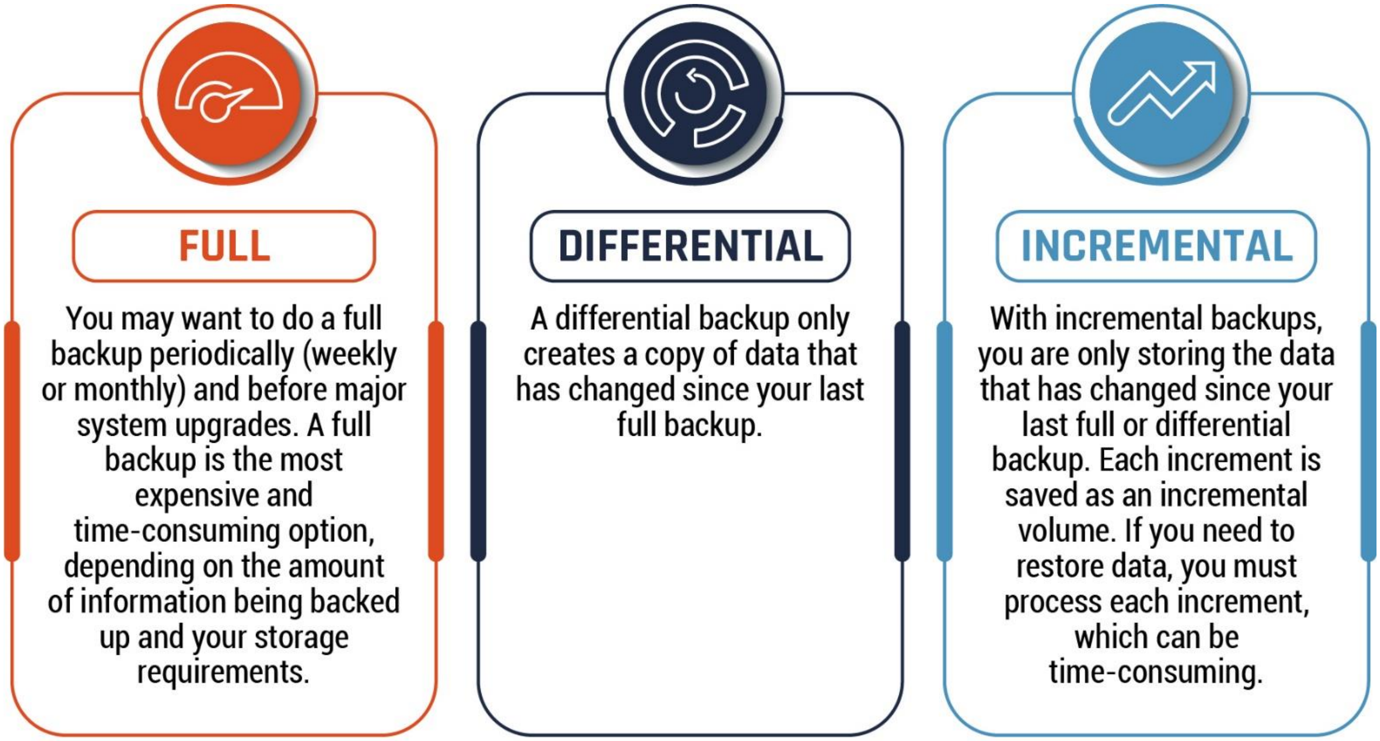
There are several approaches you can take to enhance the protection of your networks and devices. The following list of items provides details on several security controls you can implement to effectively enhance your cyber security posture.

2.1.1 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 various types of backups you can implement to protect your organization's information. Figure 3 explains the different types of backups.

Figure 3: Types of Backups



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

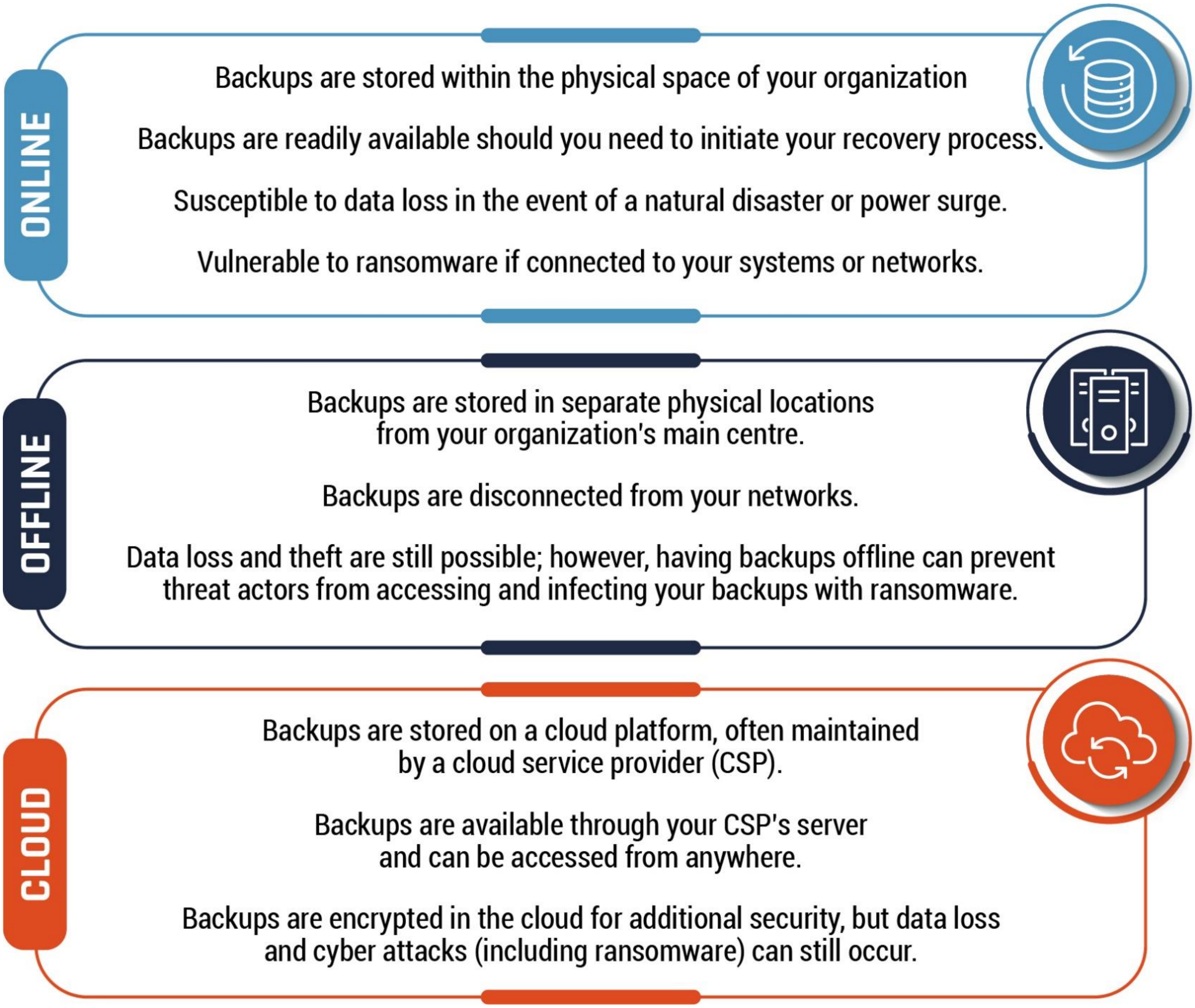
A differential backup only creates a copy of data that has changed since your last full backup.

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.

As shown in Figure 4, there are three options for storing your backups: online, offline, and cloud. Online backups are stored on a remote server or computer that is connected to your network. Unlike online backups, offline backups (“cold backups”) remain unconnected to your network and devices. Cloud backups are stored on a cloud platform maintained by a service provider.

Figure 4: Backup Options



ONLINE

Backups are stored within the physical space of your organization

Backups are 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 are stored in separate physical locations from your organization's main centre.

Backups are disconnected from your networks.

Data loss and theft are still possible; however, 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).

Backups are available through your CSP's server and can be accessed from anywhere.

Backups are encrypted in the cloud for additional security, but data loss and cyber attacks (including ransomware) can still occur.

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.

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 cloud service provider (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 two 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 (e.g. monthly). Having one or more backup files available provides your organization with an increased chance of recovering and getting back to business faster if you are the victim of ransomware, or any other cyber incident.

For more information on developing your backup plan, see *ITSAP.40.002 Tips for Backing Up Your Information* [5].

2.1.2 DEVELOP YOUR 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 business. Through these two plans, your organization considers major events that could cause an unplanned outage and 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 practised plan will help you make good decisions under the pressure of 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 shareholders and customers; and,
- Learning from incidents identifies gaps and issues with your response capability

There are several key elements to your incident response plan. The main goal is to recover from an incident in the least amount of time possible. The following checklist (Table 1) 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 does provide a structured approach and action items your organization can implement. By including the elements from Table 1 in the early development stages of your incident response plan, you can ensure you 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 faster.

For more information on developing your incident response plan, see *ITSAP.40.003 Developing Your Incident Response Plan* [6].

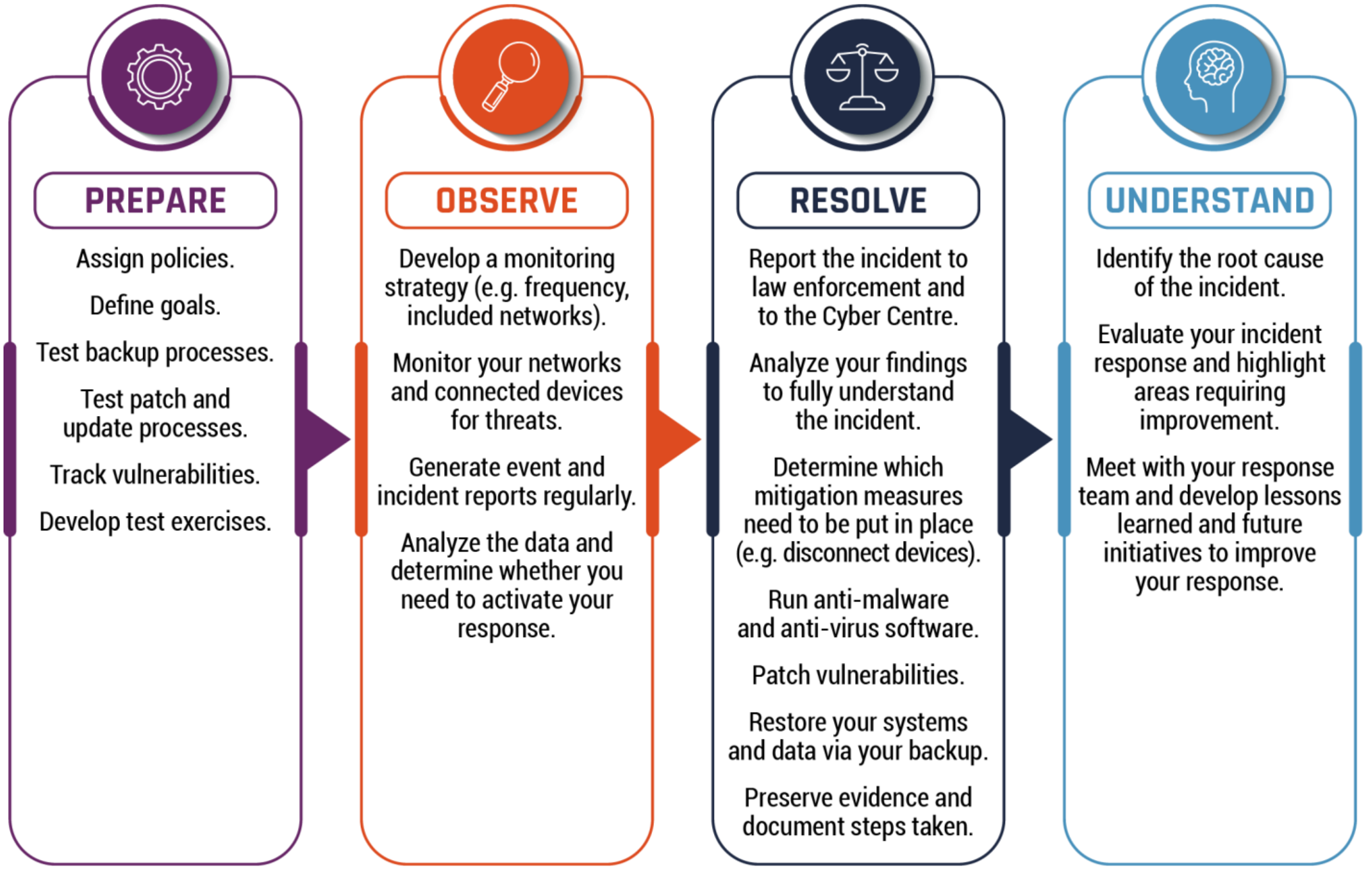
Table 1: Incident Response Plan Checklist

PRIORITY	ELEMENT	REQUIREMENTS
1.	RISK ASSESSMENT	☐ Identify your 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.
2.	POLICIES & PROCEDURES	☐ Develop an incident response policy that establishes the authorities, roles, and responsibilities for your organization. ☐ Ensure pre-authorizations to contract assistance are established and communicated to key incident response contacts.
3.	ESTABLISH YOUR CYBER INCIDENT RESPONSE TEAM (CIRT)	☐ Create a CIRT to assess, document, and respond to incidents, restore your systems, recover information, and reduce the risk of the incident reoccurring. ☐ 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.
4.	TRAINING	☐ Tailor your training programs to your organization’s business needs and requirements, as well as your employees’ roles and responsibilities. ☐ Ensure your training includes the cyber security controls listed in section 2.2 (e.g. spotting malicious emails and phishing attacks and using strong passwords or passphrases). ☐ Consult the Cyber Centre Learning Hub for advice and guidance on cyber security event management training. The Learning Hub offers a comprehensive event management course that can be tailored to our organization’s business and IT needs.

5.	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 managed service providers. Depending on the incident, you may need to contact law enforcement or a lawyer.
6.	COMMUNICATIONS	☐ 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 response team, key personnel, and key stakeholders. ☐ Prepare sample media statements that can be tailored to cyber incidents as they occur. ☐ Consider retaining a third party organization who can guide you through your incident response and recovery process.

Your incident response process will follow a lifecycle in the four phases identified in Figure 5. You can use these phases to structure your plan and your response. A primary part of your incident response should include reporting cybercrimes to law enforcement (e.g. your local police department or the Canadian Anti-Fraud Centre), and online via the Cyber Centre's My Cyber Portal.

Figure 5: Incident Response Phases



PREPARE

Assign policies.

Define goals.

Test backup processes.

Test patch and update processes.

Track vulnerabilities.

Develop test exercises.

OBSERVE

Develop a monitoring strategy (e.g. 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.

RESOLVE

Report the incident to law enforcement and to the Cyber Centre.

Analyze your findings to fully understand the incident.

Determine which mitigation measures need to be put in place (e.g. disconnect devices).

Run anti-malware and anti-virus software.

Patch vulnerabilities.

Restore your systems and data via your backup.

Preserve evidence and document steps taken.

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.

2.1.3 DEVELOP YOUR RECOVERY PLAN

Your recovery plan should complement your incident response and backup plans. When developing your recovery response, you should consider many variables and clearly identify and document what is to be recovered, by whom, when, and where. Consider the following guidelines detailed in Table 2 when developing your recovery plan:

Table 2: Guidelines for Your Recovery Plan

PHASE	GUIDELINE
PLANNING	□ Identify stakeholders including clients, vendors, business owners, systems owners, and managers. □ Identify your response team members, as well as 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 required participants are aware of their role 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. Your policy may add an additional layer of protection and may also provide your organization with incident response expertise in the event of a ransomware attack.
MEASURE	□ Set clear recovery objectives. □ Define backup and recovery strategies. □ Test your plan.
COMMUNICATIONS	□ Develop a communications plan to inform key stakeholders. □ Develop a training program for employees to ensure everyone is aware of their roles, responsibilities, and order of operations during an incident. □ Connect with your managed service providers (MSPs) to identify areas in which 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 information may include financial records, proprietary assets, and personal data. Critical applications are the systems running your key business functions and are imperative to your business. These are the systems you need to restore immediately to have 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 (e.g. cyber attack, significant power outage, or natural disaster) to help you identify key participants and stakeholders, address the significant risks, develop mitigation strategies, and identify the 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. During 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, see *ITSAP.40.004 Developing Your IT Recovery Plan* [7].

2.1.4 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 (e.g. access to email and limited access to internal systems) to reduce the risk of ransomware infecting your administrator accounts and system access that is 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.

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, and access sensitive information. Attackers can also learn which detection and recovery activities are in place on your systems, helping them avoid discovery and preventing you from stopping further attacks.

To manage access to your systems and data, apply the ***principle of least privilege: 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 enable multi-factor authentication (MFA) at all access points into your network and 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 password for each privileged account;
    - Change default passwords 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; and,
- Decommission and delete user accounts when someone leaves the organization.

In addition to managing your accounts, it is also imperative that you 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, refer to *ITSAP.10.094 Managing and Controlling Administrative Privileges* [8] and *ITSAP.30.032 Best Practices for Passwords and Passphrases* [9].

2.2 CYBER SECURITY CONTROLS

When implementing and maintaining a defence-in-depth defence model, it is imperative that your organization layers security controls throughout your networks to protect the security, confidentiality, integrity, and availability of your networks, devices, and information.

The following diagram (Figure 6) once again highlights the three stages of a ransomware incident: the threat actor gains access to your network, takes control of your systems and connected devices, and then deploys the malware payload and infect your systems and connected devices with ransomware. As shown in Figure 6, a variety of security controls, layered throughout your networks, can enhance your ability to defend against ransomware.

Note: Some cyber security controls identified in Figure 6 can be applied at various stages or areas within your network and systems. For example, logging and alerting and network segmentation are applied at all layers of your defence-in-depth strategy.

In the first stage of a ransomware incident, 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 preferable 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 and 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.

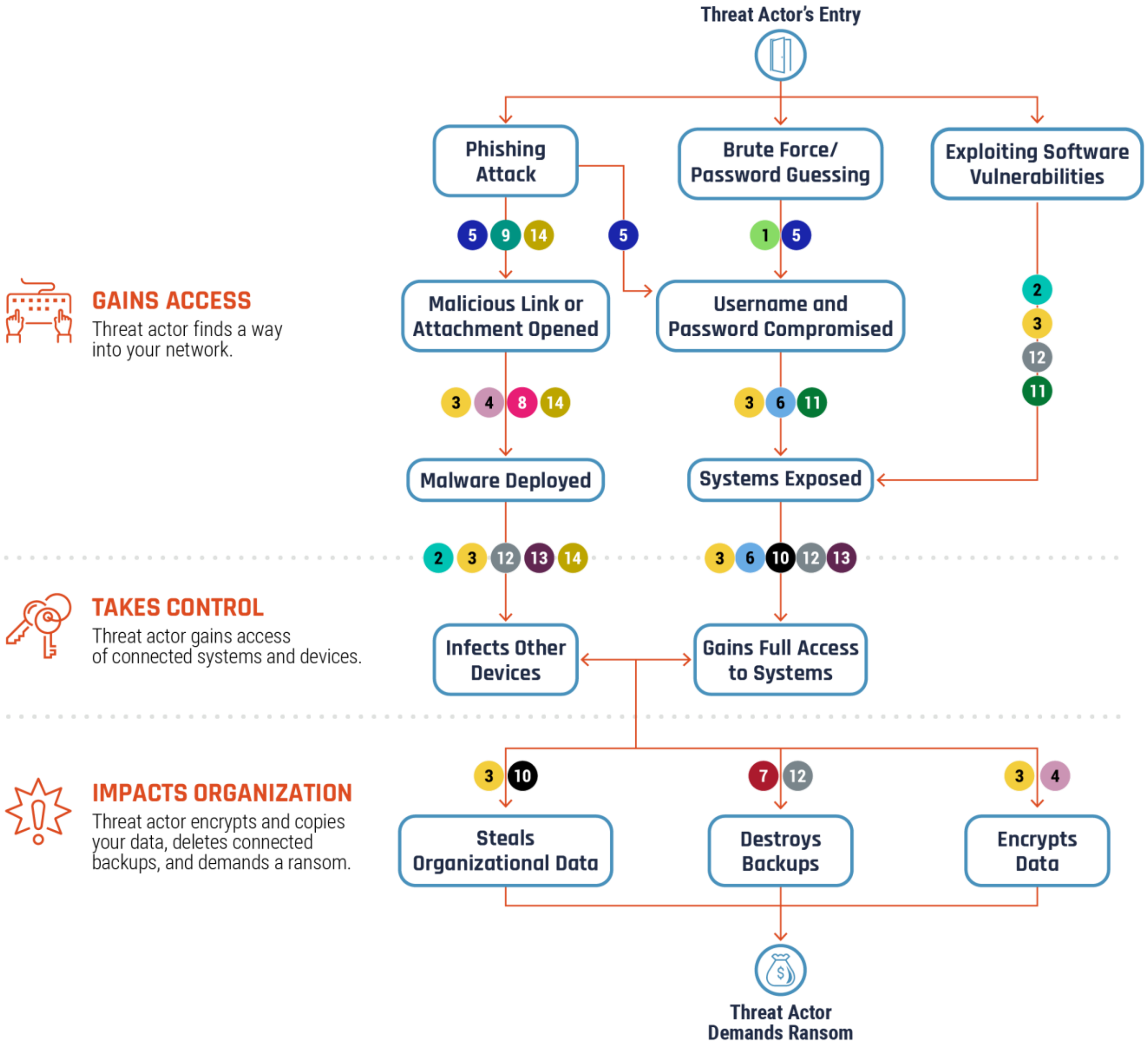
- Setup monitoring and logging functionality for your systems and networks and ensure you receive automated alerts if any anomalies are detected.
- Protect your systems that are connected or exposed to the Internet with encryption, firewalls, MFA, and frequent vulnerability assessments.
- Disable macros to decrease the risk of ransomware being spread through Microsoft Office attachments.

In the second stage of a ransomware incident, there are some mitigation measures you can implement to enhance the protection of your systems and networks and prevent ransomware from spreading across your network and connected devices.

- Implement security tools, such as anti-virus and anti-malware software, as well as 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, the number one mitigation measure you can implement for your organization is your backup plan. Ensure you have multiple copies of your backup 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 backups and restore processes on a regularly scheduled basis 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.

Figure 6: Security Controls to Reduce the Risk of Ransomware [10]


Threat Actor's Entry
Phishing Attack
Brute Force/ Password Guessing
Exploiting Software Vulnerabilities
5 9 14
5
1 5
2 3 12 11
GAINS ACCESS
Threat actor finds a way into your network.
Malicious Link or Attachment Opened
Username and Password Compromised
3 4 8 14
3 6 11
Malware Deployed
Systems Exposed
2 3 12 13 14
3 6 10 12 13
TAKES CONTROL
Threat actor gains access of connected systems and devices.
Infects Other Devices
Gains Full Access to Systems
3 10
7 12
3 4
IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.
Steals Organizational Data
Destroys Backups
Encrypts Data
Threat Actor Demands Ransom

MITIGATION TOOLS

1	Password Manager	8	Disable Macros
2	Updating and Patching	9	Email Domain Protection
3	Logging and Alerting	10	Principle of Least Privilege
4	Application Allowlisting	11	Secure Systems Exposed to the Internet
5	Cyber Security Training	12	Network Segmentation
6	Multi-Factor Authentication	13	Security Tools (e.g. Anti-virus, Anti-malware, Firewall)
7	Backups	14	Protective Domain Name System (DNS)

The following section provides more detailed guidance on the various security controls your organization can implement.

For more information on security controls, see *Baseline Security Controls for Small and Medium Organizations* [11] and *ITSAP.10.035 Top Measures to Enhance Cyber Security for Small and Medium Organizations* [12].

2.2.1 ESTABLISH PERIMETER DEFENCES

Protecting your network, connected systems and devices against cyber threats can seem like a daunting task. Perimeter defences to protect the boundary between two network security zones through which your traffic is routed. If this is defended by basic security protocols like firewalls, anti-virus and anti-malware software, your overall protection is significantly enhanced. Installing anti-phishing software is another option for enhancing your organization's cyber security. Anti-phishing software blocks phishing emails to prevent attacks from occurring or spreading further.

Ensure your users access your network using your 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 two points, such as your laptop and your organization's network.

For more information about VPNs, refer to *ITSAP.80.101 Virtual Private Networks* [13].

2.2.2 IMPLEMENT LOGGING AND ALERTING

Implementing continuous monitoring of your networks will help you establish a baseline for acceptable activity patterns within your organization. Establishing monitoring capabilities for your networks and systems can help your organization manage risk. Your monitoring system should generate logs that can be reviewed by IT specialists and management when necessary. Access to your logs should be limited to those who need to review them.

Implementing automatic alerting within your monitoring practices is also necessary in order for anomalies in activity patterns to be flagged and reviewed, as well as potential vulnerabilities and events that need risk mitigation action to be taken. The alerts will indicate something out of the ordinary has occurred and 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. They should be a stamp in time and assist you in understanding what led to an event or an incident.

If your organization becomes a victim of ransomware or another type of cyber incident, your logs could provide you with insight into how the incident occurred and what controls or mitigation measures can be implemented to better protect your networks and systems from future incidents.

2.2.3 CONDUCT PENETRATION TESTING

Penetration testing is a method for gaining assurance of the security of a system. During a penetration test, the tester attempts to breach some or all of the system's security, using the same tools and techniques that an adversary may use. It is not meant to be a primary method of identifying vulnerabilities, rather a method of ensuring your organization's vulnerability assessment and management processes are effective.

2.2.4 SEGMENT YOUR NETWORKS

When segmenting your network, you divide your networks into smaller sections or zones. With network segmentation, traffic is directed and flows through the different sections of the network. Segmenting your network 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 control and restrict access to your information. When segmenting your network, ensure your information technology (IT) and operational technology (OT) networks are identified, separated, and monitored. 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.

2.2.5 CONSTRAIN SCRIPTING ENVIRONMENTS AND DISABLE MACROS

If your organization is using Windows, you may want to consider constraining your scripting environments. With Windows specifically, Microsoft developed an automated system administration capability through an interface powered by their shell scripting language (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 [14]. 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 the threat actor's code injection will typically not be blocked by anti-virus or anti-malware software or by your systems' event logs.

Another item to consider when using Windows is macros in Microsoft Office applications. Macros are written sequences that imitate user keystrokes and mouse commands to automatically repeat tasks in applications. Macros are used in many 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 (e.g. sort worksheets alphabetically, unmerge all merged cells, 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 disable macros and ensure users are not able to re-enable disabled macros. You should also ensure 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, refer to *ITSAP.00.200 How to Protect Your Organization from Malicious Macros* [15].

2.2.6 PATCH AND UPDATE

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

1. **Bug fix patch**: Repairs functionality issues in software (e.g. error that causes unexpected device behaviour);
2. **Security patch**: Addresses security vulnerabilities to protect the system from threats (e.g. malware infecting devices through security flaws); or
3. **Feature patch**: Adds new functions to the software (e.g. enhancements to application performance and speed).

For more information on patching and updating your devices, see *ITSAP.10.096 How Updates Secure Your Devices* [16].

2.2.7 CREATE AN APPLICATION ALLOW LIST

Application allowing involves the creation of an access control list that identifies who or what is allowed access, in order to provide protection from harm. An allow list selects and approves specific applications and application components (e.g. executable programs, software libraries, configuration files) to run on organizational systems. Application allow lists help 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 an application is launched, it is compared against the allow list. The application is only permitted if it is on that list. Hashing is used to verify the application's integrity, meaning the application is what it says it is. Hashing generates a value from a string of text and 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.

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

2.2.8 USE PROTECTIVE DOMAIN NAME SYSTEM (DNS)

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

Protective DNS is a tool that can be implemented by your organization to block employees using corporately issued devices from visiting potentially malicious domains on the internet. 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 your organization's network.

You should also consider implementing protective DNS filtering on any mobile devices used by employees of your organization, 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. Canadians can use a free public DNS application called Canadian Shield provided by the Canadian Internet Registration Authority (CIRA) to ensure personal devices always use a trusted DNS and filter out malicious IP addresses [17]. Canadian Shield can be set-up on your router or gateway to better protect your entire network.

It is recommended to apply their "Protected" DNS resolver as it is designed to offer enhanced malware and phishing blocking functionality. By replacing the default DNS server settings on your devices with a trusted DNS server you can better protect your devices.

2.2.9 APPLY PASSWORD MANAGEMENT

When permitted, your organization should consider implementing passphrases in place of passwords, however, most systems are set up to require a username and password to grant access. Using strong passwords is one 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.

Section 2.1.4 provides details on adopting MFA into your account and access management practices. In conjunction with MFA, implementing the use of a password manager for your staff members can be a beneficial tool in remembering and securing passwords required to access your networks and systems. Password managers can be a useful tool for your organization to keep track of the numerous passwords for individual and administrative accounts.

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

For more information on the implementation and use of password managers, see *ITSAP.30.025 Password Managers – Security* [18].

2.2.10 USE EMAIL DOMAIN PROTECTION

Consider implementing technical security measures to protect your organization's domains from email spoofing, preventing the delivery of malicious messages sent 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 three security protocols that act jointly to protect email domains from being spoofed:

- **Sender Policy Framework (SPF):** You can use SPF to specify the Internet protocol (IP) addresses from which emails can be sent on a domain's behalf. When a message is received, an email system that supports SPF will retrieve the SPF record that is associated with the sending domain and verify that the IP address used to send the message has been authorized to do so.

- **DomainKeys Identified Mail (DKIM):** You can use DKIM to provide a mechanism for email messages to be authenticated using a cryptographic signature. 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.

- **Domain-based Messaged Authentication, Reporting and Conformance (DMARC):** Implementing DMARC policy and verification can enhance your security protocols and protect your email domains from being spoofed. 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 marked as suspicious, or reject the email.

Your organization should understand these policies and what they will do. Only a rejection policy will prevent illegitimate messages from being delivered. For more information on email domain protection, see *ITSP.40.065 Implementation Guidance: Email Domain Protection* [19].

3 HOW TO RECOVER FROM RANSOMWARE

Recovering from ransomware can be a lengthy process and recovering your organization's brand and reputation can be an even longer process. Working on the assumption that your organization will encounter some form of malware will assist you in developing 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 it can also reduce the likelihood of an attack occurring or minimize the impact of an infection.

3.1 RECOVERY PROCESS

As described in subsection 2.1.3, 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.

3.1.1 IMMEDIATE RESPONSE ACTIONS

Threat actors can infiltrate your network and continue to have visibility into your systems, connected devices, and communications. You should assume the threat actor has visibility into your organization and therefore you should implement an alternative communication method (e.g. external email accessed by a device not connected to your network) that is not accessible to them. This will also block the threat actor from gaining insight into your intended incident response plans and recovery actions. Below, we provide a checklist (Table 2) for your organization to follow when taking immediate action, ideally within the first few hours, against a ransomware attack.

Table 3: Immediate Response Checklist – Detection, Analysis, Containment, and Eradication

PRIORITY	ACTION ITEM	DETAILED STEPS
1.	DETERMINE WHAT IS INFECTED AND ISOLATE	□ Determine which devices and systems are infected with the ransomware. □ Isolate all infected systems and devices. □ Disconnect the infected systems and devices from any network connection to reduce the risk of the infection spreading to other connected devices. You may also need to disconnect them from the Internet. □ Determine what data, even in-transit data, has been impacted by the ransomware. □ Establish the likelihood of the confidentiality or integrity of the data being compromised and inform data managers and stakeholders of potential impacts. □ You may also need to disable your virtual private networks, remote access servers, single sign on resources, and cloud-based or public-facing assets as additional measures to contain the ransomware infection.

2.	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. □ Law enforcement may be able to provide you with a decryption key if you have been infected with a known type of ransomware.
3.	ASSEMBLE 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 assist your CIRT with where to focus immediate actions.
4.	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 may lock you out of systems needed during the recovery process. □ Create temporary administrator accounts to begin your recovery and monitor whether your original accounts are being leveraged by the threat actor.
5.	WIPE & REINSTALL	□ Safely wipe your infected devices to remove any malware, bugs, or viruses. □ Reinstall the operating system to rid your devices of the infection.
6.	RUN SECURITY SOFTWARE	□ Run anti-virus and anti-malware diagnostics on your backup to make sure it is clean before you begin the restore process. □ Scan any files that might have been accessed by the threat actor or extracted from a compromised system. See the Cyber Centre's website to download our free malware detection and analysis tool Assemblyline [20]. □ Address any items flagged by the scans.

3.1.2 RECOVERY ACTIONS

Despite temporary disruptions to your business, isolating your infrastructure from the Internet is the most important course of action. Isolation will temporarily remove the threat actor's access to you infrastructure, allowing you to gain control and further your incident investigation, response, and recovery.

Once you have completed the steps identified in Table 2, and you are positive that both your backups and your devices are clear of any malware or viruses, you should begin your recovery process, as outlined in subsections 3.1.2.1 to 3.1.2.4.

3.1.2.1 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 connecting your systems or devices to your network or the Internet to thwart the threat actor's ability to gain access in the same manner.

3.1.2.2 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 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 to ensure it hasn't been compromised by the threat actor.

3.1.2.3 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.

3.1.2.4 ENGAGE CYBER SECURITY PROFESSIONAL ASSISTANCE

Procuring professional services from a highly rated cyber security agency or professional can be a helpful asset 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 a 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.

3.1.2.5 INFORM STAKEHOLDERS

When an incident occurs, and especially when it compromises your systems and data, it is imperative you inform key stakeholders, clients, and your staff members. You should consider preparing a statement in advance that can then 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 to ensure your stakeholders are informed and able to enact their own incident response plans if necessary.

3.1.2.6 ANALYZE THE INCIDENT

Determining the root cause of the incident is key. How did the threat actor gain access to your network and deploy the ransomware? Often the ransomware incident is a symptom of a more serious hack or intrusion by the threat actor. Without identifying how they gained access and applying appropriate security measures to prevent it from happening again, threat actors may continue to exploit the vulnerability.

Determining what systems, accounts, and information have been accessed by the threat actor is a vital step in your incident analysis. This will enable you to determine the extent of the damage, such as what accounts were compromised and what data was exfiltrated, which will inform your approach to control the attack, prepare, and implement a proper response, and execute a successful recovery.

4 SUMMARY

Ransomware is an ever-present threat to your organization. It can have devastating impacts on your business, often halting your ability to produce products and services. Ransomware incidents can also cause you to incur financial loss, data breaches, and reputational damage to 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 method to implement further mitigation measures and correct 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 (e.g. local police or the Canadian Anti-Fraud Centre) as well as 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 enable the Cyber Centre to provide alerts and guidance to the public, to help individuals and organizations protect their assets from the same ransomware attack. Sharing your lessons learned can benefit other organizations and the cyber security community.

4.1 CONTACT INFORMATION

For more information, you can phone or email our Services Coordination Centre:

Service Coordination Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

5 SUPPORTING CONTENT

5.1 LIST OF ABBREVIATIONS

Term	Definition
BIA	Business Impact Analysis
CIRT	Cyber Incident Response Team
CSP	Cloud Service Provider
DKIM	DomainKeys Identified Mail
DMARC	Domain-Based Message Authentication, Reporting, and Conformance
GC	Government of Canada
IT	Information Technology
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
OS	Operating System
OT	Operational Technology
RaaS	Ransomware as a Service
RDP	Remote Desktop Protocol
SPF	Sender Policy Framework
SSO	Single Sign-On
VPN	Virtual Private Network

5.2 GLOSSARY

Term	Definition
Administrative Privileges	The permissions that allow a user to perform certain functions on a system or network, such as installing software and changing configuration settings.
Allow List	An access control list that identifies who or what is allowed access, in order to provide protection from harm.
Backdoor	An undocumented, private, or less-detectible way of gaining remote access to a computer, bypassing authentication measures, and obtaining access to plaintext.
Cloud Computing	The use of remote servers hosted on the Internet. Cloud computing allows users to access a shared pool of computing resources (such as networks, servers, applications, or services) on demand and from anywhere. Users access these resources via a computer network instead of storing and maintaining all resources on their local computer.
Defence-in-Depth	An IT security concept (also known as the Castle Approach) in which multiple layers of security are used to protect the integrity of information. These layers can include antivirus and antispyware software, firewalls, hierarchical passwords, intrusion detection, and biometric identification.
Firewall	A security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside.
Least Privilege	The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.
Macros	A small program that can automate tasks in applications which attackers can use to gain access to (or harm) a system.
Multi-Factor Authentication	Authentication is validated by using a combination of two or more different factors including: something you know (e.g. a password), something you have (e.g. a physical token), or something you are (a biometric).
Network Security Zone	A networking environment with a well-defined boundary, a Network Security Zone Authority, and a standard level of weakness to network threats. Types of Zones are distinguished by security requirements for interfaces, traffic control, data protection, host configuration control, and network configuration control.
Perimeter	The boundary between two network security zones through which traffic is routed.
Phishing	An attempt by a third party 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.
PowerShell	A powerful shell scripting language developed by Microsoft to provide an integrated interface for automated system administration.
Spoofing	A threat actor uses the Internet Protocol (IP) address of another computer to masquerade as a trusted source to gain access to an individual’s or organization’s computer, device, or network.

5.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSM.50.030 Cyber Security Considerations for Consumers of Managed Services*. October 2020.
2	Canadian Centre for Cyber Security. *ITSAP.00.070 Supply Chain Security for Small and Medium-size Organizations*. March 2019
3	CERT NZ. *How ransomware happens and how to stop it – Lifecycle of a ransomware incident.* September 2021.
4	Canadian Centre for Cyber Security. *National Cyber Threat Assessment 2020*. November 2020.
5	Canadian Centre for Cyber Security. *ITSAP.40.002 Tips for Backing Up Your Information*. October 2020.
6	Canadian Centre for Cyber Security. *ITSAP.40.003 Developing Your Incident Response Plan.* May 2021.
7	Canadian Centre for Cyber Security. *ITSAP.40.004 Developing Your IT Recovery Plan*. January 2021.
8	Canadian Centre for Cyber Security. *ITSAP.10.094 Managing and Controlling Administrative Privileges*. July 2020.
9	Canadian Centre for Cyber Security. *ITSAP.30.032 Best Practices for Passwords and Passphrases.* September 2019.
10	CERT NZ. *How ransomware happens and how to stop it – Lifecycle of a ransomware incident.* September 2021.
11	Canadian Centre for Cyber Security. *Baseline Security Controls for Small and Medium Organizations*. February 2020.
12	Canadian Centre for Cyber Security. *ITSAP.10.035 Top Measures to Enhance Cyber Security for Small and Medium Organizations*. June 2021.
13	Canadian Centre for Cyber Security. *ITSAP.80.101 Virtual Private Networks*. October 2019.
14	Australian Cyber Security Centre. *Securing PowerShell in the Enterprise*. June 2020.
15	Canadian Centre for Cyber Security. *ITSAP.00.200 How to Protect Your Organization from Malicious Macros*. September 2020.
16	Canadian Centre for Cyber Security. *ITSAP.10.096 How Updates Secure Your Devices.* March 2021.
17	Canadian Internet Registration Authority (CIRA). Canadian Shield.
18	Canadian Centre for Cyber Security. *ITSAP.30.025 Password Managers – Security*. September 2019.
19	Canadian Centre for Cyber Security. *ITSP.40.065 Implementation Guidance: Email Domain Protection*. August 2021.
20	Canadian Centre for Cyber Security. Assemblyline.