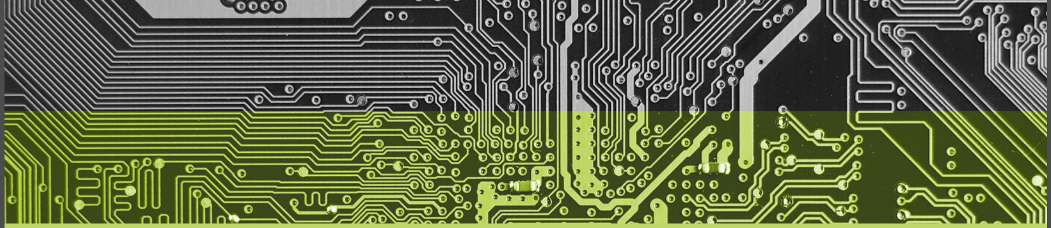

UPDATED OCTOBER 2022

TECHNOLOGY

FACT SHEET

How to Protect Against Ransomware

Ransomware is a top threat facing Ontario organizations. Ransomware attacks can destroy vital records, knock out critical systems and services, and put sensitive information into the hands of criminals.

Organizations subject to Ontario's access and privacy laws must ensure that their cybersecurity programs include reasonable measures to protect their information holdings. This fact sheet is meant to be a useful overview for organizations and the people they serve.

This guide by the Office of the Information and Privacy Commissioner of Ontario (IPC) is for informational purposes only and should not be relied upon as a substitute for the legislation itself, or as legal advice. It is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws. It does not bind the IPC's Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit **www.ipc.on.ca**.

WHAT IS RANSOMWARE?

Ransomware attacks involve the digital extortion of an organization. Attackers gain control of an organization's data holdings and often threaten to take damaging action unless they receive payment. Most ransomware attacks involve at least one of the following tactics:

- **Lock out.** Attackers gain control of business-critical systems, file repositories, and backups. They also use tools such as encryption to lock an organization out of its own information and systems, refusing to restore access until they receive payment.
- **Data theft.** Attackers gain access to large volumes of information, copy these records to a location they control, and threaten to publish them unless they receive payment.

The Canadian Centre for Cybersecurity **reports** having knowledge of 235 ransomware attacks that affected Canadian organizations in 2021. The actual number is thought to be much higher because of underreporting. For example, a **2022 TELUS survey** of 463 Canadian businesses found that 83

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

per cent of respondents have experienced an attempted ransomware attack. An **August 2022 survey** by the Canadian Internet Registration Authority found that the number of organizations that had fallen victim to a successful ransomware attack had risen over 40 per cent in the past year, from 17 per cent to 24 per cent.

IMPACTS OF RANSOMWARE

Ransomware attacks can lead to serious harms, including those caused by breaches of privacy, leaked confidential records, lost access to records, or the disruption of systems and services.

For individuals and communities

- **Harms to health, safety, and public order**. Large-scale service outages of IT systems in organizations that provide essential services have led to **cancelled surgeries** in hospitals and first responders **losing emergency dispatch access**.
- **Distress.** Uncertainty about what information has been stolen or who has access to it can leave individuals feeling helpless or distressed. This is especially true where the information is sensitive and its release could lead to harm to the individual, such as when it relates to **survivors of domestic violence** or recipients of mental health services.
- **Financial loss**. Stolen credit card information along with other personal and financial information are often the targets of a ransomware attack for use in identity fraud schemes.
- **Inability to exercise access to information rights.** Lost government records and personal information can make it difficult for individuals to access their information and hold organizations accountable for their practices and decisions.

For organizations

- **Interruption of internal functions**. **Government institutions**, including municipalities, have lost access to information necessary to provide services or carry out internal operations because of ransomware attacks.
- **Reputational harm.** Twenty-five per cent of respondents to a **2021 survey** of Canadian public and private sector cybersecurity decision-makers whose organizations experienced a ransomware attack said the attack resulted in reputational harm to their organization.
- **Loss of employee trust.** Internal records containing **sensitive employee information** are often included in ransomware attacks, and may negatively affect employer/employee relationships.

- **Financial loss**. Organizations can **lose revenue** when payment or client information systems are encrypted, or locked down or otherwise unavailable due to a ransomware attack.

LEGAL OBLIGATIONS TO SAFEGUARD AGAINST RANSOMWARE

Organizations subject to Ontario's access and privacy laws[1] must take reasonable steps to protect information[2] they hold from unauthorized access and disclosure, and unauthorized or inadvertent disposal or destruction. Health information custodians and child and family service providers are also required to protect personal information against unauthorized use, copying, and modification, and against loss and theft. They must also ensure that personal information is retained, transferred, and disposed of in a secure manner. [3]

The lifecycle of a ransomware attack generally involves several stages. The following are examples of how unauthorized access or use, or the loss or theft of personal information might occur during one or more of these stages.[4]

Access

Ransomware attackers typically use software tools to remotely control a legitimate user account belonging to the target organization. Attackers then move through their target's IT environment. They often **process lists of files and records** to understand the target organization's information holdings. Attackers may not necessarily examine or view each record, but will try to gain or make use of the information to steal and/or encrypt it.

Use

Ransomware attackers will typically use this access to attack an organization's information holdings. They may use this information to pressure the target organization to pay a ransom. For example, attackers will often copy records from various organizational systems into a **staging area** and from there compress the files for easier transmission. They may also input information into an encryption program that **transforms the**

[1] The ***Freedom of Information and Protection of Privacy Act*** (FIPPA); ***Municipal Freedom of Information and Protection of Privacy Act*** (MFIPPA); ***Personal Health Information Protection Act*** (PHIPA); Part X of the ***Child, Youth and Family Services Act*** (CYFSA).

[2] This fact sheet uses the term 'information' to mean any information that organizations are required to protect under Ontario's access and privacy laws. This includes government records under FIPPA/MFIPPA, and personal information and personal health information as defined in FIPPA/MFIPPA, PHIPA and CYFSA. This fact sheet uses the term 'personal information' to refer to both personal information and personal health information, but excludes government records that are not personal information under FIPPA or MFIPPA.

[3] **O Reg 460**, s. 4 (1) and 4(3); **O Reg 823**, s. 3 (1) and 3 (3); **PHIPA**, s. 12(1) and s. 13(1); **CYFSA**,s. 308 (1) and s. 309 (1).

[4] These examples are provided for informational and guidance purposes. They are not intended to be an exhaustive or definitive discussion of the ways in which an organization's obligation to protect personal information may be impacted by ransomware attacks.

information into illegible data that can only be interpreted using a secret key controlled by the attacker.

Loss

In most circumstances, if a ransomware attacker encrypts information held by an organization, the organization is unable to access and use it. Such information would not be available should the organization need it to provide a service or undertake a key function. Organizations may also be unable to respond to requests for access to the encrypted information. Even if an organization is able to recover information from backups, the incident may nonetheless be considered a loss of that information.

Theft

Ransomware attacks often involve the unauthorized transmission of information outside of an organization (otherwise known as "exfiltration"). In these instances, attackers copy information and use it for unlawful purposes. Information removal during a ransomware attack would generally be considered a theft of that information.

INFORMATION SECURITY ACCOUNTABILITY

The above examples show why organizations subject to Ontario's access and privacy laws must have reasonable measures in place to protect against ransomware attacks. To help your organization meet its security obligations, the IPC recommends that you:

- **Create a foundation for accountability.** Having reasonable measures in place to identify, protect, detect, respond, and recover from threats such as ransomware requires organizational commitment and internal oversight. This could include the establishment of a privacy and security governance committee consisting of senior executives responsible for information technology, legal services, access, and privacy.
- **Formalize accountability** in an overarching information security policy. That policy should set out roles, responsibilities, reporting mechanisms, and requirements for putting in place technical, administrative, and physical safeguards. This can help your organization keep pace with emerging risks such as ransomware.
- **Implement accountability** by ensuring the measures defined in your information security policy have been put into practice and are being followed. This could include regular monitoring, testing, or auditing of those practices.
- **Maintain accountability** when using service providers by establishing contractual obligations to demonstrate their compliance with cybersecurity best practices, including those outlined in this document, and immediately report breaches or suspected breaches to your organization as soon as they become aware of them.

- **Improve accountability** by continually strengthening your security program. This includes evaluating the effectiveness of the measures you have implemented and adapting your security program to changing circumstances.

SECURING YOUR ORGANIZATION

Your organization can reduce the likelihood and impact of successful ransomware attacks by having a strong cybersecurity program. There are key steps that you should take to protect your organization from a ransomware attack.

Know your assets and information holdings across their entire lifecycle

Taking reasonable steps to protect information from ransomware attacks requires a clear understanding of your organization's information holdings.[5] This includes maintaining records of the sensitivity, volume, and nature of your organization's various information holdings. You should document where your information is stored. This applies to cloud computing environments as well as other service providers who process information on behalf of your organization.

Your organization should:

- **Maintain an asset inventory** that tracks where and how information flows through your organization, such as IT systems (servers, workstations, mobile devices) connected to your organization's network, what information is stored in those systems, program areas accountable for the information stored in those systems, hardware and software version information, and contact information for responsible IT administrators.
- **Classify and label information and IT assets** according to sensitivity (the level of harm that could result from a loss of confidentiality, integrity, or availability of this information). Put in place safeguards proportionate to sensitivity classification levels.
- **Put in place a risk management program** that establishes requirements for regular security assessments of both in-house IT systems and third party service providers. This can include vulnerability scans, penetration tests, threat/risk assessments, and privacy impact assessments.
- **Ensure personal information and sensitive records are securely disposed** of according to retention schedules and media disposal requirements.

[5] For instance, the IPC's **Privacy Compliant Report PR16-40** notes that "[d]epending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions."

Understand the threats and mitigate them

Your organization should maintain an up-to-date understanding of the ransomware threat landscape. Ransomware attacks may involve sophisticated criminal enterprises that are continuously innovating their methods.

There are several steps your organization can take to improve its security at key stages during a typical ransomware attack.[6]

Initial Access

Your organization should have safeguards in place to prevent and detect the methods ransomware attackers use to get initial access to a network and take further actions.[7] The most common initial access methods used in ransomware attacks are:

- **Social engineering attacks**. An attacker communicates with a person who has access to the target network and manipulates them into performing an action that allows the attacker to take control of their computer or user account. These attacks commonly originate with phishing emails, misleading websites, and online advertisements. The point is to lure employees into installing malicious software or providing passwords or other login details.
- **Exploiting vulnerabilities in systems connected to the internet**. Attackers scan the internet to discover and send malicious software instructions to systems that have not been patched or configured to address known vulnerabilities. This may include attacks such as brute force password guessing, where an attacker uses automated means to try millions of different passwords in an attempt to find one that will grant access. These types of attacks commonly target an organization's infrastructure that supports remote access, email, and web applications, or poorly configured cloud storage platforms.
- **Supply chain compromise**. Sophisticated attackers can compromise third party products or services used by your organization to get direct access into your network. For example, attackers can insert malicious code into open source software libraries,[8] or compromise remote administration tools used by IT service providers.[9]

[6] This fact sheet is not intended to serve as a complete accounting list of a ransomware attacker's actor tools, tactics, and procedures.

[7] Organizations should not assume ransomware threats originate externally, ignoring the possibility of malicious internal actors. Consider, for instance, **this breach** (non-ransomware) that impacted nearly 10 million individuals in Canada and abroad.

[8] Open source software is often developed in public view and members of the public can often contribute code changes that make their way into software releases. Open source code is widely used in popular technologies and leading cloud services. In a **2020 report**, leading open source software platform GitHub reported that for a random sample of open source code on their platform, 17% of vulnerabilities in that code appear to have been deliberately introduced for malicious purposes (e.g., to facilitate later attacks).

[9] Many organizations hire third party companies as "managed IT service providers," who remotely perform functions traditionally performed by in-house IT staff. These service providers often use software tools to remotely manage their clients' IT infrastructure. These

Your organization should take proactive steps to reduce the risk of attackers gaining access to your organizational IT systems, including the following:

- **Put in place email security controls** to detect and prevent the delivery of emails with suspicious links, malicious attachments, and spoofed sender addresses. See the IPC's ***Protect Against Phishing*** fact sheet for more information.
- **Establish a vulnerability management program** to:
    - Subscribe to technical advisories about the latest vulnerabilities affecting your organization's IT environments (including third party service providers).
    - Scan your organization's systems for the presence of vulnerabilities.
    - Apply patches or other solutions as soon as possible.
    - Prioritize vulnerabilities that ransomware attackers are known to exploit.
- **Follow system hardening best practices.** Hardening generally involves reducing the number of pathways that an attacker can take to get access to your network. For example, the following are steps your organization can take to harden its systems (including cloud environments):
    - Disable unused IT services.
    - Restrict who can install software and run custom scripts.
    - Limit end users' ability to launch Microsoft Office macros.
    - Ensure computers are configured consistently using standardized system images. System images can be used to automate the setup of new systems to ensure that appropriate security settings are put in place and security applications installed.
- **Develop strategies to mitigate risk to systems that are out of date** such as regularly replacing systems that can only operate on vulnerable versions of operating systems or web application frameworks.
- **Restrict employee access** to suspicious websites.
- **Ensure that all employees receive up-to-date cybersecurity awareness training** that includes content about ransomware attacks and how they occur.

management tools are often authorized to install software, manage configuration, and perform other sensitive operations. Such remote management tools are attractive targets for cyber threat actors. Several high profile breaches, such as the **2021 Kaseya ransomware attacks**, have been linked to compromised remote management tools that were used by attackers to infiltrate hundreds of organizations.

- **Install security tools** on all computers that can prevent malware, quarantine suspicious files, and issue alerts, such as enterprise antivirus tools or endpoint detection and response tools.
- **Use good authentication practices** including **effective passwords**, password management, strong multi-factor authentication, and limiting password reuse. Organizations should also keep up with advances in authentication, such as a shift to the 'no-password' approach.

Privilege escalation and lateral movement

Attackers generally use their initial access as a foothold to gain access to other systems on the IT network. They often exploit vulnerabilities in the system to gain administrator privileges and use common IT management tools to access and control large volumes of sensitive information or block the delivery of critical services.

To limit an attacker's movement in the network, your organization should:

- **Follow the 'principle of least privilege.'** Start from the assumption that users should have limited rights to access and perform limited functions on computer systems. You should only grant additional access and authorizations that are necessary for the user to perform their specific duties and responsibilities. Consider adopting **a zero-trust approach** to cybersecurity.
- **Minimize and monitor the use of administrator accounts.** For example, administrator accounts should not be used for regular office tasks. Organizations should also consider access management tools that can grant temporary privileges upon request.
- **Segregate IT assets** into different network security zones. For example, an organization could create separate zones for public-facing application servers, internal databases, and employee workstations. Network activity between these zones could then be monitored or limited.
- **Develop a baseline** of typical network and endpoint activity and put in place measures to identify irregular traffic that could suggest attacker movement.

Encryption and data theft

Once ransomware attackers have access to an organization's network and have gained control of information and systems, they may then threaten to destroy records or publicly disclose sensitive information. Attackers also regularly target backups and live systems to undermine an organization's ability to recover from the attack.

To help your organization detect, prevent, and recover from a ransomware attack:

- **Maintain regular backups** of information and systems in an offline environment.
- **Monitor the integrity of records** for irregular changes to large numbers of files or to highly sensitive information.
- **Detect the unauthorized use of tools and application programming interfaces** (APIs) that encrypt data.
- Use data loss prevention tools to log, monitor, and block network traffic of irregular file transfers to untrusted destinations or known file upload websites.
- **Configure computers** (user workstations, servers, and cloud infrastructure) **beyond default settings** to **log a wide range of events and information**. Actions that will help to ensure breach investigations have access to more detailed information include:
    - Taking steps to prevent logs from being modified, overwritten, or deleted without authorization after they are created.
    - Developing a retention schedule for event logs.
- **Combine event logs** from across your organization's IT assets (including cloud infrastructure) into a centralized location. Consider using a security information and event management solution to develop a clearer picture of a ransomware attacker's activity.

Respond to cybersecurity incidents

Taking timely steps to assess cybersecurity incidents and ensuring procedures are in place to respond to actual and suspected breaches are critical components of any cybersecurity program. Several IPC decisions have established that having a breach response plan in place is an important part of the reasonable measures an organization must have to protect the information it holds.[10] This includes establishing a formal cybersecurity incident management program that has at least the following components:

- **Identification** of roles and responsibilities, training, and clear senior leadership accountability for identifying and responding to cybersecurity incidents.
- **A dedicated cyber incident response team** that includes senior management, IT (including third party service providers, where appropriate), as well as legal, communications and human resources staff, as needed.

[10] For example, **PHIPA Decision 110** notes that "[t]he duty to take reasonable steps to protect personal health information includes a duty to respond adequately to a complaint of a privacy breach. Among other things, a proper response will help ensure that any breach is contained and will not re-occur." **Privacy Complaint Report PR16-40** further discusses some considerations for cyberattack incident response, including the expectation that security alerts and reports be thoroughly investigated in a timely manner.

- **Criteria** to identify and classify cybersecurity incidents and privacy breaches in a consistent manner according to their nature and severity.
- **Procedures and timelines** for internal communications and escalation according to the nature and severity of the incident.
- **Processes, procedures, and technology tools** for incident detection and analysis, containment, eradication, recovery, and remediation.
- **Clear authorization** to disconnect critical systems from the network, disable user accounts, and other decisive actions to contain the incident.
- **Clear procedures** for determining when to report incidents to regulators and law enforcement.
- **A communications plan** that addresses how your organization will communicate with employees, affected individuals, the public, and other stakeholders about the incident.

The cybersecurity incident management program should also include specific documented plans and procedures to handle ransomware attacks. These plans should include:

- **Maintaining a list of qualified cybersecurity firms** (or having such a firm on retainer) that can assist on short notice with a forensic investigation (including investigating the dark web for signs that data has been published online), remediation, and, if necessary, cautiously interacting with the attackers.
    - Procedures should include the circumstances for when the firm will be engaged, including for what types of incidents, and at what point in the incident response process.
    - The retained firm should follow the best practices outlined in this fact sheet, and commit to provide evidence of their investigation to regulators and law enforcement if a breach investigation is opened.
    - Procedures for analyzing network logs to determine if data removal (exfiltration) has occurred.
- **Developing general business continuity and disaster recovery plans** that include:
    - Procedures for the secure and timely restoration of files and systems from backups and system images, and the routine testing of such procedures.
- **Consider obtaining a cyber insurance policy** that offsets the costs associated with responding to an incident such as forensic investigations, legal fees, data recovery services, and financial fraud.

Privacy breach notification

When cybersecurity incidents, including ransomware attacks, involve personal information, they may also constitute privacy breaches within the meaning of Ontario's laws. In such cases, health information custodians and child and family service providers will generally be required,[11] and provincial and municipal institutions are strongly recommended, to:

- **Notify affected individuals.** Determine the identity of the individuals whose personal information was affected by the ransomware attack and notify them of the breach.
- **Report to the IPC.** Report ransomware attacks to the Office of the Information and Privacy Commissioner of Ontario. You can **report a breach online** or reach us at 1-800-387-0073 or **info@ipc.on.ca**. For more guidance on privacy breach response and notification, please consult these IPC resources:
    - ***Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector***
    - ***Responding to a Health Privacy Breach: Guidelines for the Health Sector***
    - ***Privacy Breaches: Guidelines for Public Sector Organizations***
    - ***Reporting a Privacy Breach to the Information and Privacy Commissioner: Guidelines for Service Providers***

Adapt to changing circumstances

What is reasonable in one situation might not necessarily be reasonable in another. When it comes to security safeguards, organizations must adapt to changing circumstances and keep their cybersecurity management program evergreen.[12]

To better adapt to evolving threats, including ransomware, your organization should:

- **Operate a cybersecurity threat intelligence program** that proactively monitors the evolving threat landscape and exchanges information with other organizations. This program should also identify strategic and tactical opportunities to protect against threats and reduce risk exposure.
- **Conduct privacy and security risk assessments** whenever major new technology changes are introduced, and ensure that all critical elements of your IT environment are regularly reassessed.

[11] PHIPA, s, 12(2) and 12 (3) and CYFSA, s. s. 308 (2) and (3). Reports to the IPC are required when a theft, loss, or unauthorized use or disclosure of personal information meet certain prescribed requirements.

[12] Former Commissioner Brian Beamish stated in **Order HO-013** with respect to security measures required under PHIPA: "As new technologies are developed, adopted or implemented and as new threats and vulnerabilities emerge, 'steps that are reasonable in the circumstances,' the standard in section 12(1) of the Act, will also evolve."

- **Ensure that incident response plans and cybersecurity policies and procedures are regularly reviewed**, tested, and updated for new threat developments.
- **Ensure that lessons learned from ransomware attacks are identified** and any corrective actions are put in place in a timely manner to prevent similar incidents in the future.

Align with industry standards and best practices

Keeping up to date with industry standards and best practices is important in determining if your organization has reasonable safeguards in place.[13] Frameworks and standards to consider include the National Institute for Standards and Technology (NIST) **Cybersecurity Framework**, the International Organization for Standardization's **Information Security Management** standard (ISO/IEC 270001), and the Center for Internet Security **Critical Security Controls**.

These cybersecurity frameworks don't provide a one-size fits all approach. Instead, these frameworks often set out different categories of security goals. Organizations may choose to invest more heavily in particular security areas than in others, based on their assessed risk profile, strategic direction, and legal obligations.

The IPC strongly recommends that organizations adopt an industry standard cybersecurity framework and further invest in measures that best address serious threats such as ransomware. For example, the U.S. NIST has a **quick start guide** that identifies which categories of its cybersecurity framework need particular investment to protect against ransomware.

TAKE IMMEDIATE AND PROACTIVE STEPS TODAY

Your organization can take immediate steps to improve its security posture by:

- **Immediately identifying and mitigating vulnerabilities in internet-connected systems known to be exploited by cyber attackers**. To get started, consider prioritizing vulnerabilities included in the annual list of the **top routinely exploited vulnerabilities** maintained by the U.S. Cybersecurity and Infrastructure Security Agency in collaboration with the Canadian Centre for Cyber Security. You should initiate incident response procedures if you find that your network contains routinely exploited vulnerabilities that have not already been mitigated in a timely manner.
- **Conducting a tabletop exercise**. Invite senior leadership to take part in a role-playing or simulation exercise that explores the steps staff should take in response to a ransomware attack. These exercises can be inexpensive and efficient tools to flag serious gaps

[13] For example, Order **HO-010** notes the standard of reasonableness includes having regard for "evolving industry standards and practices, and the technical safeguards employed by other hospitals in the province."

in security measures. They can also help advance the business case for investments that support cybersecurity.

- **Subscribing to or implementing an employee training program** to teach employees about the risks of phishing and how to identify suspicious emails, avoid falling prey to tactics, and immediately report potential risks to IT. Consider sending occasional mock phishing emails to employees as a way of strengthening their reflexes.
- **Joining cybersecurity information sharing networks.** The Community of Practice Network coordinated by the Ontario government's **Cybersecurity Centre of Excellence** offers cybersecurity resources and support to the broader public sector.

LEARN MORE

Cyber Security Ontario Learning Portal

Canadian Centre for Cyber Security: Ransomware playbook (ITSM.00.099)

National Cyber Security Centre (UK): A guide to ransomware

Cybersecurity and Infrastructure Security Agency: Stop Ransomware

Cybersecurity and Infrastructure Security Agency: Tabletop Exercises Packages

NIST Cybersecurity Framework

Center for Internet Security

CIO Strategy Council: Baseline cyber security controls for small and medium organizations

Microsoft Security Best Practices: What is ransomware

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario