Ryerson University | ROGERS cybersecure catalyst | corporate training and cyber range

Ransomware Tip Sheet Technical Advisors

What is ransomware?

There are various forms of ransomware, but in general, ransomware is a type of malicious software that a cybercriminal uses to encrypt or lock your digital files or software. Once the ransomware is installed, the cybercriminal then typically demands a ransom to unencrypt the files or software and restore your access. The size of the ransom can vary.

How does it happen?

Ransomware can be installed in your systems several ways. One of the most common is for a cybercriminal to find a vulnerability or weakness in your system through which they can gain access and install the ransomware. Another common way is through a phishing email, text or phone call that appears to be legitimate. The email or text will entice the user to click on a link, open an attachment, provide system access or information that will facilitate installation of the ransomware.

Why should you be concerned?

As a Technical Advisor within your organization, you may be consulted by senior leadership or your IT or security team on what actions to take. Your advice can help ensure that the organization is taking appropriate preventative measures and that it is sufficiently prepared to respond to a ransomware attack, thereby minimizing the impact.

What can you do about it?

There are measures you can take that will help you **prevent** and **prepare** for a ransomware attack.

Prevent – Things you can do to help prevent ransomware include:

- **Enhance and promote good IT and Operational Technology (OT) practices.** Regardless of the systems used, there are common practices that help keep you secure such as keeping operating systems up-to-date and software patched, continuous monitoring for system anomalies, maintaining and reviewing logs, keeping an up to date asset inventory, turning off remote desktop protocol if it's not needed, managing passwords, and ensuring regular system and software back ups.
- **Ensuring that security software is installed and activated on all endpoints.** This will help protect organizational systems and devices. It may also help detect ransomware and could stop emails or texts with malicious files. Consider advanced threat protection if it is available through your system or service provider.
- **Establish cyber security policies and procedures** in your organization that follow principles of least privilege, support rigorous access controls, and limit abilities to download or install unauthorized applications.
- **Identify your own and employee training requirements.** For you, it just makes sense to be up to speed on the latest threats and what you can do about them. For employees, the training should be focused on helping them to recognize common signs of phishing and other social engineering techniques and what to do if they detect suspicious activity. This should include a reporting process so they know who to call in the event they encounter ransomware. If you are attacked, the organizational actions will depend largely on the type of attack and what's at risk. Any actions should be in consultation with the organizational leaders.

Ryerson University | ROGERS cybersecure catalyst | corporate training and cyber range

If you are attacked, the organizational actions will depend largely on the type of attack and what's at risk. Any actions should be in consultation with the organizational leaders.

Prepare – You should be prepared to respond to a ransomware attack by:

- **There is an incident response plan** that includes specific roles and responsibilities throughout an incident including crisis and communications management. Your incident response plan should include ransomware scenarios, and should be exercised and tested at least annually through a Tabletop Exercise to identify gaps and ensure that everyone understands their roles and responsibilities.
- **First responders are aware of and capable of performing their tasks.** Whether you have an in-house IT or cyber security team or you are using third party services, incident response activities should be coordinated and all members of the response team should be competent in fulfilling their role. This should include readily available procedures (e.g. a playbook) to support technical response actions. Remember these should be available offline in the event of a ransomware scenario.
- **You've identified required expertise and tools** to support ransomware response, removal and system recovery. Whether you have in-house expertise or use a third-party service, you should be confident that they have the skills and tools needed to support mitigations and recovery activity. Ensure that critical contact information is available outside of systems you use as you may not have access to them if you are locked out.
- **Your systems are backed up.** You should be backing up files, systems and software often in a location segregated from your operating and administrative networks to avoid them being held hostage as well. If possible, the back ups should be encrypted. Liaise with system owners or business line managers to understand the value of their data and their work flows to help determine back up frequency and the level of additional protections that might be required. Ensure that full and partial backups are regularly tested and that they are accurate, effective and uncorrupted.
- **Detailed, technical recovery protocols in place** so that there is no confusion on recovering from back ups and that team members who will be supporting recovery operations are well versed in their tasks. This should include the opportunity to practice restore and recovery procedures.
- **Ensuring there's a process for you and your team to report the incident** to appropriate organizational authorities and, when required, to the Canadian Anti-Fraud Centre, the Canadian Centre for Cyber Security and, if personal information is compromised, the local Privacy Commissioner.

Contact us or visit our website to learn more and keep up-to-date on our Ransomware role-based training products and events.

Rogers Cybersecure Catalyst Corporate Training & Cyber Range program offers a variety of training options, from introductory cybersecurity concepts to complex technical experiences.

Our training offerings are versatile and can be tailored to meet the specific needs of our clients and include interactive workshops and Tabletop Exercises.