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

Ransomware Tip Sheet IT and Cyber Security Operations Professionals

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 an IT or cyber security professional within your organization, you are on the frontlines of this type of incident and will be expected to act to minimize the impact on the organization. You may also advise on any part of the incident response process including prevention, remediation and recovery activities.

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:

- **Apply IT and Operational Technology (OT) best 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.
- **Ensure that security software is installed and activated on all end points.** This will help protect organizational systems and devices. It may also help detect ransomware and could stop emails or texts with malicious files. If advanced threat protection is available, understand how it can be leveraged.
- **Identify and resolve vulnerabilities.** Reducing vulnerabilities that can be exploited will help decrease your exposure and deny opportunities to threat actors who attempt to gain access to your systems.
- **Encourage cyber security best practices.** In your interactions with users, help them learn about cyber security best practices and things that they can do to help prevent and respond to ransomware.
- **Get the training you need.** You are critical to your organization's cyber security. Ensure that you have the skills you need to help prevent, prepare for, detect, respond and recover from a ransomware attack.

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 a risk. Any actions should be in consultation with the organizational leaders.

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

- **You understand your role and are prepared to act.** This means that you should have the training and tools needed to be able to effectively respond to and help mitigate a ransomware attack. This may include training on specific tools or techniques to help remove ransomware or working with other specialists on mitigation and recovery.
- **You exercise technical response activities.** In addition to the organization practicing incident response procedures, the technical team should ensure they can confidently respond to incidents such as ransomware. You and your team should be exercised in ransomware scenarios and that not only give the opportunity to practice your skills, but help assess team workflows and communications within the team and with other parts of the organization.
- **You've identified required expertise and tools** to support ransomware removal and system recovery. You may not have the knowledge and skills to support full response and recovery. Whether you have in-house expertise or use a third-party service, you should be confident that the organization can obtain the resources required for mitigations and recovery activity. Ensure that critical contact information is available outside of systems you use as you may not have access to them during a ransomware attack.
- **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. 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 are in place** so that there is no confusion on recovering from back ups and that and that team members who will be supporting recovery operations are well versed in their tasks. This should include the opportunity for you to practice restore and recovery procedures in which you may play a role.

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.