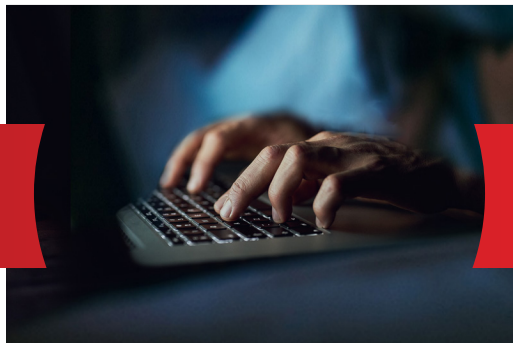

How to reduce ransomware attacks against your organization

Cybercriminals are escalating attacks against critical infrastructures, including hospitals and healthcare systems, utility companies and government agencies. Organizations need to be prepared to act now to protect systems and sensitive data against an attack.

What is Ransomware?

According to the FBI's 2022 Internet Crime Report, adjusted losses of more than $34.3 million were reported from ransomware attacks. Ransomware is a growing threat to all organizations—regardless of size, industry, or sector. With several recent high-profile attacks impacting healthcare and hospital systems around the country, there have been impacts on patient care and postponement of surgeries.

Ransomware is a form of malware that targets vulnerabilities in an organization's computer network system and uses encryption to hold a victim's personal information for ransom. Criminals will steal and encrypt data, locking users from accessing files, databases, or applications.

Often, criminals will demand a ransom payment for the decryption key that will provide access to those files and information or threaten to release the stolen data. However, paying the ransom does not always mean criminals will release the files to the target and an organization can still be locked out for weeks or even months. In some cases, paying a ransom payment is illegal. Ransomware enables criminals to continue funding and launching attacks against other companies.

Ransomware is commonly delivered through phishing emails, which appear to be sent from a legitimate organization or someone known to the victim, enticing the user to click on a malicious link or open an attachment. Once the user clicks on the link, the malware spreads throughout the organization's system undetected and allows the cybercriminal to launch an attack later. Criminals also deliver brute force attacks against an external system, such as remote desktop protocol services, to exploit vulnerabilities in a computer network and gain access.

How to Reduce Ransomware Attacks

What can your organization do to reduce the risk of a ransomware attack? It starts at the top by implementing a culture of awareness. Executives can adopt a heightened security mindset and create a culture to ensure staff are regularly trained on how to protect valuable assets, such as payment platforms and sensitive data.

(continued)

The FBI's Internet Crime Complaint Center and the Cybersecurity & Infrastructure Security Agency (CISA) offer best practices and prevention tips for all employees—including those working in technology, payments, and on other teams—to help strengthen controls and defenses against ransomware attacks.

- **Back-up your data and systems.** Regularly evaluate your back-ups and make an offline copy of your data (e.g., separate from your personal computer). If your computer becomes infected with ransomware, you can restore systems to their previous state using your back-ups.
- **Update and patch operating systems and software.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.
- **Use multifactor authentication.** Use multifactor authentication (e.g., password + pin code) vs. just a password on your devices.
- **Use caution when clicking on links or opening attachments.** Be careful when clicking directly on links in emails, even if the sender is someone you know. Never use the contact information contained in an email signature to verify.
- **Schedule regular training for employees and test response plans.** Conduct phishing exercises to raise awareness and help spot the warnings signs for suspicious emails. Test response times from Security/IT teams to help mitigate and respond to reduce exposure from a potential attack.

What to Do If Your Organization is Impacted?

For additional best practices to prepare, respond to and mitigate the impact from a cyberattack on your organization, please visit CISA's website.

If you would like to request an MUFG cybersecurity speaker, please contact your Relationship Team.