RANSOMWARE:
Reduce the Risk to Your Business

Ransomware is a type of malicious software that can encrypt all your files until you pay a ransom to regain access.

Why Should I Care About Ransomware?

The impact of a ransomware attack is high. Ransomware infections are expensive and cause significant business disruption. In Q1 2021, the average ransom payment was $220,298 and victims were down for 23 days. This does not include costs to investigate and recover, nor the costs to implement security safeguards to prevent another infection. Other impacts include lost data, lost employee productivity, lost revenue, reputational harm, and brand erosion. Even if your data was backed up, it still costs time and money to get your business back online.

Is My Business Really a Target?

With current trends, the likelihood of a business being infected by ransomware is medium-high. Most ransomware attacks are aimed at businesses of all sizes, although only the larger attacks make the headlines. Sophisticated cybercriminals are selling ransomware-as-a-service (RaaS) kits that enable those without much technical knowledge to conduct attacks. Two-thirds of ransomware infections analyzed during 2020 came from cybercriminals using RaaS. While the more technically savvy tend to attack larger entities, like governments and large businesses, RaaS kits increase the likelihood that cybercriminals will infect small businesses and organizations. Also, small businesses and organizations are often easier to successfully infect as they rarely have all the security safeguards that larger entities do.

RANSOMWARE:
Reduce the Risk to Your Business

Reducing the Risk

Your risk related to ransomware depends on your vulnerabilities, the likelihood of your business getting infected, and the impact if it did. Here are some steps you can take to reduce vulnerabilities and thus the likelihood of being infected by ransomware, as well as steps to reduce the impact if your business is infected. If needed, work with your IT provider to implement these steps.

Reducing the Likelihood

- Keep your software up-to-date; patch security vulnerabilities quickly. If possible, turn on auto-update features to ensure your computer, operating system, website, tablets, and smartphones are running the most current software. Check your device or software maker, like Apple and Microsoft, for instructions on how to turn on auto-update.
- Implement multi-factor authentication (MFA) on the accounts used to access computers, phones, social media, email, and other systems and applications. An example of MFA is when you must enter a code sent to your smartphone after you enter your password to log in. Passwords alone are no longer enough to protect computer accounts.
- Implement anti-malware programs to detect and respond to malicious software. Those suitable for businesses are known as endpoint detection and response (EDR) tools.
- Train your computer users at least quarterly not to click on unexpected email attachments or links. About 60% of ransomware incidents start with a malicious email, according to the Cybersecurity and Infrastructure Security Agency (CISA).

Reducing the Impact

- Periodically back up your information, test the backups to ensure they work, and store them offline. Many types of ransomware try to find and encrypt or delete backups that are connected to the network, which means that copies of your data stored in the cloud are vulnerable. If you do not have a cloud backup solution, back your data up to a thumb drive, DVD, or CD and store it in a locked, fireproof safe or cabinet. As a rule of thumb, if you have to plug something in or log in to access your backup, then it should be safe from ransomware.
- Ensure you have an incident response plan and support, so you know what to do and who to contact if attacked. Print a copy of the plan just in case you cannot access your computer or network. Review and update your incident response plan regularly.
- Consider purchasing cyber insurance to transfer your risk.
- If you are attacked with ransomware, contact your local FBI Field Office. They may be able to help you recover, and information about your attack might help prevent others from getting infected.

For More Information

There are several online resources to help you reduce your risk of ransomware. Here are a few to get you started:

- Hacked computer or tablet (ransomware) from FightCyberime.org: https://fightcybercrime.org/hacked-computer-or-tablet-ransomware/
- Cyber Resource Catalog keyword search for "ransomware": https://fightcybercrime.org/cyber-resource-catalog/
- Ransomware guidance and resources from the Cybersecurity and Infrastructure Security Agency (CISA): https://www.cisa.gov/stopransomware
- The U.S. government's guide, How to Protect Your Networks from Ransomware: https://www.justice.gov/criminal-ccips/file/872771/