RETAIL & HOSPITALITY ISAC

Protecting Your Business from Ransomware Attacks

Ransomware, a type of malicious software that infects and restricts access to a computer until a ransom is paid, affects businesses of all sizes. Ransomware groups seek to conduct computer intrusions, exfiltrate sensitive data, destroy backups, and then encrypt critical system files so they are not accessible to their owner without a complex encryption key. The key is then made available for sale – typically for a seven-figure sum. This type of attack is among the most pervasive malware threats, with thousands of incidents happening to businesses each day.

The good news is that there are best practices you can adopt to protect your business. The following are recent recommendations from U.S. government cybersecurity experts for easily reducing the risk of computer intrusion and ransomware. This list is not exhaustive, but implementing these reasonable security measures can make ransomware incidents less likely for franchise owner/operators.

Require Multi-Factor Authentication

Passwords alone are routinely compromised. Turning on multi-factor authentication for your systems is one of the simplest ways you can deter attacks. MFA should be employed for all services if possible, but particularly web-mail, virtual private networks, and accounts that access critical systems.

Backup Your Data

- Make sure your data, system images, and configurations are regularly backed up and that backups are tested.
- Keep backups offline, not connected to the business networks, so they can't be encrypted or deleted in the event of an attack.
- Encrypt your data to prevent use if stolen.

Update and Patch Systems

- Use endpoint detection and response to identify and block malicious network activity.
- Consider using a centralized patch management system to automate patch management and keep all systems up to date in a timely manner. A delay in patching puts your business at immediate increased risk.
- Prioritize timely patching of internet-facing servers and software processing internet data.

Segment Your Networks

- Ransomware attacks are no longer just about stealing data. Attackers want to disrupt your operations. The average business downtime caused by a ransomware attack in 2021 is 23 days.
- Segmenting your networks so that a shutdown of corporate business functions doesn't also shut down your manufacturing/production operations is vital.
- Filter and limit internet access to operational networks.
- Identify links between networks and develop manual controls to continue operation in the event of a compromise.

Educate Your Team

- Implement a security awareness training program. Phishing emails are a common entry point for ransomware attackers that can be easily averted with safe employee behavior.

Test Your Incident Response Plan

- First, make sure that you have an incident response plan in place and that key stakeholders throughout the company are involved.
- Conduct a vulnerability scan to identify areas of your system most likely to be targeted.
- Run through some core questions such as, how long are you able to sustain business operations without access to these systems?
- Test specific scenarios to practice real-time decision-making.
- Make improvements based on identified gaps in planning.

Check Your Security Team's Work

- Similar to testing your incident response plan, you should also be checking your cybersecurity program as a whole.
- Penetration testing can be conducted by a third-party partner to identify vulnerabilities that your team may not be aware of.
- Penetration testing is less costly than a breach and can provide an outside perspective and additional skillsets to your program.