

# RANSOMWARE: PREVENTION AND PROTECTION

## REAL-TIME PROTECTION

Ransomware is a growing threat since malicious actors have found ways to monetize malware paralyzing computer systems and demanding a ransom be paid for their release. Unlike other malware, which often has to stay hidden for long periods of time to operate effectively, ransomware is engineered to execute quickly through spear-phishing, compromised websites, and corrupted downloads. Financial institutions are particularly vulnerable to the impact of ransomware because these attacks can threaten the ability to move funds quickly and efficiently and because they are considered lucrative targets. However, bad actors sometimes break their promises: even after a ransom is paid, some attackers do not remove the malware or release confidential data.

- Invest in anti-malware protection systems that adapt to new threat intelligence in real-time.
- Evaluate the security of all devices connected to networks that house sensitive or essential information. Connect all nonessential systems to a separate network.
  - Be particularly careful when bringing IoT or “smart devices” into your workspaces, since these systems often have weaker or nonexistent security systems and can be targeted as access points to essential systems.
  - Consider the security of remote work setups. Ensure security tools work off-network to monitor all web traffic.
- Promote employee education around phishing attacks and the necessity of strong password protections.
- Consider implementing multifactor authentication across your organization if feasible.
- Keep all systems and software regularly updated. Change settings to allow for automated updates if possible.
- Develop an incident response and crisis management plan for how to deal with a ransomware attack and the loss of valuable data.
- Prepare an external communication plan in the event of a ransomware attack.

## DATA BACKUPS

- Invest in secure, regularly updated backup systems that keep your data protected.
  - If using USBs or hard drives, physically disconnect these devices from networked computers after backups are finished.
  - If using cloud storage, equip server with high-level encryption and multifactor authentication.
- Create a read-only copy of the general ledger for worst case disaster recovery.
- Develop systems that perform automated data recovery and remediation.
- Develop scenarios to assess how long it will take to recover critical data and business services.

## REGULATORY ENVIRONMENT

- Evaluate the relevant regulatory and legal guidance for ransomware in your operating environment.
  - Consider country-specific guidance. Develop a plan for periodic evaluation of changing guidance.
  - Consider financial-sector specific guidance.
  - Consider international legal and regulatory requirements.
- Assess risks involved with paying a ransom. In some cases, paying a ransom could violate existing sanctions regimes in place against hostile actors.
- Liaison with local law enforcement. Build connections for quick information sharing in the event of an attack.
- Assess the benefits and drawbacks of cyber insurance policies for ransomware.

## Gauging Your Organization's Ransomware Readiness

Consider the following questions when developing a ransomware prevention and protection plan.

- Does your organization have **regularly scheduled backups**?
  - Are these backups disconnected from your network, either via cloud storage systems or air-gapped USBs/hard drives?
- Are any **nonessential devices** connected to your organization's network?
  - Can they be moved to other networks that do not house sensitive data?
- Does your organization understand the **regulatory and legal risks** involved with paying a ransom?
  - Legal guidance on this varies from country to country and is frequently updated.
- Does your organization regularly update its software and systems? Are updates **automated**?
- Does your organization have a **plan for how to deal with a ransomware attack** and the loss of valuable data?
- Does your organization have a **cyber insurance policy**? If so, how does that plan cover ransomware attacks?
  - Some plans explicitly prohibit ransom payments, while others will cover such a payment as part of the policy.