

# RANSOMWARE CHECKLIST

## RANSOMWARE READINESS

- ☐ **As you develop a ransomware prevention and protection plan, periodically assess the following:**
  - Does your organization have regularly scheduled backups?
  - Are any nonessential devices connected to your organization's network?
  - Does your organization understand the regulatory and legal risks involved with paying a ransom?
- Does your organization regularly update its software systems? Are these updates automated?
- Does your organization have a plan to deal with a ransomware attack and data loss?
- Does your system have a cyber insurance policy? If so, how does that plan cover ransomware attacks?

## REAL-TIME PROTECTION

- ☐ **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.
  - ☐ 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 software and systems 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 servers 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.
  - ☐ Consider financial-sector specific guidance.
  - ☐ Consider international legal and regulatory requirements.
  - ☐ Develop a plan for periodic evaluation of changing guidance.
- ☐ Assess risks involved with paying a ransom.
- ☐ Liaise 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.