COMMERCIAL SOLUTIONS

Cybersecurity checklist

Below are some tips to help prepare and protect your organization from cyberattacks.

BASIC CYBER POSTURE:

- End Point Detection and Response tool (EDR)
- Cyber insurance policy, requires Multi-Factor Authentication (MFA)

GOOD CYBER POSTURE (ADD):

- Email protection tool
- Security Operations Team (MDR) - 24x7 monitoring
- Internal Email phishing
- Security awareness training for employees

BEST CYBER POSTURE (ADD MORE):

- Vulnerability management
- Security incident and event management tool
- Annual penetration testing
- Network detection and response tool
- Digital risk management tool

Prepare

- ☐ Identify your company's high-value assets and secure those first. Identify stakeholders' roles and responsibilities in the event of a cyber event and maintain a call tree/communication list.
- ☐ Create core security policies (e.g., Acceptable Use, Data Protection, Passwords, Mobile Device).
- ☐ Enforce strong password policy (including potential changes every 90 days), do not share credentials.
- ☐ Consider security technologies that provide layered security (e.g. firewall, patch management, end-point protection, antivirus software, web email content filtering, and MFA).

Protect

- ☐ Implement a least-privilege approach to employee access to data and software installs.
- ☐ Implement a security awareness program to train employees on policies and reducing human risk (e.g., phishing, password security, data protection, online and mobile device safety).
- ☐ Perform regular and reliable data backups, test your restoration processes.
- ☐ Update software and patch systems as soon as they are available. Update versions as soon as possible.
- ☐ Assess the cybersecurity posture of vendors and include security obligations in contracts before engaging them.
- ☐ Secure a comprehensive cyber liability insurance program. Understand the insuring language, including exclusions and endorsements/addendums.

Respond

- ☐ Prepare an incident response plan to act quickly and efficiently (e.g., NIST framework can help).
- ☐ Response should include simultaneously working alongside counsel that is trained in cyber responses and your cyber liability insurer.
- ☐ Consider security technologies that assist with monitoring, detection, response, and recovery capabilities.
- ☐ Conduct simulations to identify opportunities to strengthen your security posture.

Avoid fraudulent business transactions

- ☐ Consider additional strategies to protect your organization from common types of cyber threats, especially types of fraud that can result in extensive monetary loss.
- ☐ Secure check stock, cards, and account information, monitor accounts daily and request alerts. Reconcile daily and use account alerts.
- ☐ Implement ACH blocks and filters and activate Positive Pay with your bank.
- ☐ Ensure segregation of duties for employees engaged in financial processes.
- ☐ Report suspected fraud to your local FBI office to help contain and mitigate incidents and minimize loss.
- ☐ Secure business filings with the Secretary of State and establish email alerts and password protection.
- ☐ When in doubt make a phone call and speak to a person.

BOK FINANCIAL

BOKFINANCIAL.COM/CYBERSECURITY

CM-917 04-2024