KeyBank

Take an active approach to your business security plans and controls

The constantly evolving landscape of cyberspace means big growth opportunities for hackers, criminals and terrorists. From internal correspondence to operational systems, payment systems to collection of customer data, cybercrime can be a real threat for any organization where technology impacts business operations every day. But with smart policies and consistent employee training you can stay ahead of possible risks before they develop.

KeyBank can help you take an active approach when it comes to safeguarding your business from potential fraud. Our team of experts can help your organization build a security plan by:

General best practices

- ☐ Keep informed about trends in the industry.
- ☐ Monitor your accounts frequently.
- ☐ Evaluate your policies.
- ☐ Verify your employee access rights and credentials on a regular basis.
- ☐ Review your payment types and methods.
- ☐ Utilize dual controls on payments and ensure separation of duties.
- ☐ Implement fraud prevention and mitigation solutions.
- ☐ Educate and train your employees.
- ☐ Create an environment where employees are empowered.
- ☐ Train, test, repeat.

Fraud prevention and planning best practices checklist

In addition to speaking with your banker about fraud prevention solutions, reference this helpful list of reliable fraud-prevention techniques often.

Review computer security

- ☐ Change passwords annually to maintain strong password protection and data encryption. Change passwords immediately whenever fraud is suspected.
- ☐ Ensure that antivirus programs are updated daily.
- ☐ Maintain and review your computer operating systems and web browsers.
- ☐ Install any recommended security updates as they become available.
- ☐ Limit administrative rights.
- ☐ Ensure employees lock their computers when away from their desks.
- ☐ Consider using a dedicated computer for all banking transactions.
- ☐ Use proven Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Data Loss Prevention (DLP) solutions.
- ☐ Use full encryption of Personally Identifiable Information (PII).

Set up fraud controls

- ☐ Work with IT/Security to develop a plan for responding to fraud.
  - ☐ Assemble an incident response team and prepare an incident response plan.
  - ☐ Know your company's affirmative duties and the recommended duties pursuant to state and federal laws.
- ☐ Limit the use of your ACH system to employees who need to use it.
- ☐ Use dual controls and ensure separation of duties. (E.g., use operational practices that help mitigate cybercrime risk. Wire or ACH electronic payments should be a two-person task—one to initiate the payment and one to approve it.)
- ☐ Verify employee access rights and credentials regularly.
- ☐ Ensure your vendors maintain appropriate security measures.
- ☐ Know how many records you have and what type of data is being collected, stored, shared and protected, as well as where this data resides and when it is purged.
- ☐ Utilize data classification and segmentation.
- ☐ Develop/evaluate internal fraud policies:
  - ☐ Written Information Security Program (WISP)
  - ☐ Computer and electronic devices usage
  - ☐ Document retention and destruction
  - ☐ Bring Your Own Device (BYOD)
  - ☐ Telecommuting
  - ☐ Social media
  - ☐ Website privacy and terms of use
  - ☐ Physical and logical access security
  - ☐ Confidentiality agreements for employees, vendors and visitors
  - ☐ Confirm business associate agreements are in place and that the terms and conditions relating to state and federal law compliance are appropriate and reasonable to ensure compliance with applicable laws.
- ☐ Review your employee exit process.
- ☐ Evaluate your cyber-liability insurance coverage needs.

Safeguard electronic payments—protect against fraudulent wire transactions

- ☐ Monitor all electronic payments, especially wire activity.
- ☐ Never send funds to unknown individuals.
- ☐ Develop instructions for changing any vendor payment instructions.
- ☐ Completely understand and verify any crisis or urgent requests.
- ☐ If you receive unexpected or urgent messages for funds to be wired, call the requestor at a trusted phone number to ensure they made the request.
- ☐ Discuss a contingency plan for operations with your banker in the event of a payment disruption.

Checklist continued on the following page

Approaches to risk management

Eliminate risk: Patch known exploits, encrypt laptops, etc.

Mitigate risk: Have dedicated security staff, policies, IDS/IPS, etc.

Accept risk: Employ partner Service Level Agreements (SLAs), trust partner assurances.

Cede risk: Obtain privacy risk insurance.

Communicate with and educate your employees

- ☐ Create a culture of privacy and security throughout your organization.
- ☐ Educate your employees. One-time training is not enough. Ongoing awareness and periodic testing will help keep employees on the lookout for potential fraud and in compliance with your security policies.
  - ☐ Routinely discuss how to identify fraud.
  - ☐ Communicate the risks/costs of fraud (with lessons learned from past incidents).
  - ☐ Provide ongoing data privacy and security training to your employees.
- ☐ Ensure employees are aware of and understand all internal fraud policies.
- ☐ Urge employees to read *Consumer Affairs* reports, as they often post alerts about new scams.
- ☐ Keep employees informed of new kinds of cybercrime that might infiltrate their inboxes.
- ☐ Provide a clear process through which employees can report suspicious activity and other potential cybercrime threats.

Test

- ☐ Perform a data privacy review and risk assessment, including vulnerability scanning and penetration testing.
- ☐ Conduct a Breach Response Workshop with a tabletop exercise. (E.g., your IT team can create a mock phishing attack to test employee responses, with follow-up education.)
- ☐ Perform system vulnerability testing and risk assessments.
- ☐ Test employee knowledge of processes and procedures, including how to change vendor payment instructions.

If you suspect you are a victim of fraud or malware, call Key's Fraud and Disputes Hotline directly at 1-800-433-0124 for analysis of the situation and further direction. Then contact your Relationship Manager to make them aware of the issue.

To learn more, contact your Relationship Manager, or visit key.com/security.