CYBERSECURITY FOR SMALLER ORGANIZATIONS

CISO CHECKLIST: PROTECTING YOUR CUSTOMERS

ADVISING CUSTOMERS AND EMPLOYEES ON INDIVIDUAL-LEVEL DATA PROTECTION

☐ **Provide employees and customers with the following personal guidelines to follow to better protect their data:**

- Use strong passwords on all personal and professional devices and consider using a password manager.
- Keep operating systems and other software and applications up to date on all computers and mobile devices.
- Install anti-virus, anti-malware, and anti-ransomware software that prevents, detects, and removes malicious programs.
- Use a firewall program to prevent unauthorized access to your computer.
- Only use security products from reputable companies. Read reviews from computer and consumer publications and consider consulting with the manufacturer of your computer or operating system.
- Be careful with sensitive information. Do not send bank account passwords or other sensitive financial account data over unencrypted email.
- Be smart about where and how you connect to the Internet for banking or other communications involving sensitive personal information.
- Don't immediately open email attachments or click on links in unsolicited or suspicious-looking emails. Stop. Think. Click.
- Be suspicious if someone contacts you unexpectedly online or via telephone and asks for your personal information. Even when communicating with known addresses, try to minimize sharing of personal information via email.
- Remember that no financial institution will email or call you and request confidential information they already have about you.
- Assume that a request for information from a bank where you've never opened an account is a scam.
- Verify the validity of a suspicious looking email or a pop-up box before providing personal information. Pay close attention to the email address.

ADMINISTERING ACCOUNTS

☐ **Require that customers use strong user IDs and passwords to log into your services. Advise them not to use the same password as they do for other accounts.**

☐ **Use instant verification, real-time verification, trial deposit verification, identity verification, and/or out of wallet questions to validate real customers and reduce the opportunity for fraud.**

☐ **Offer or, ideally, require two-factor authentication for customers to use when logging into your services.**

☐ **Regularly check user accounts for signs of fraud.**

PROTECTING DATA

☐ **Consider which customer data your organization must collect to perform its services, and be wary of collecting any customer data that goes beyond that.**

☐ **Set and distribute data retention policies. Dispose of customer data when no longer needed.**

☐ **Encrypt customer data in transit and at rest.**

☐ **Put in place data security policies to make clear what data transfer methods are approved versus restricted and to specify what is acceptable for all employees when dealing with customer data. Ensure that these policies are documented, communicated, enforced for all staff, and periodically reviewed and updated.**

SECURING PUBLIC WEB APPLICATIONS

- ☐ **Implement HTTPS on your organization's public-facing web application(s) and redirect all HTTP traffic to HTTPS.**
- ☐ **Use a content security policy on your website(s).**
- ☐ **Enable public key pinning on your website(s).**
- ☐ **Ensure that your public-facing web application(s) never use cookies to store highly sensitive or critical customer information (such as passwords) and that they have conservative expiration dates for cookies (sooner rather than later).**
- ☐ **Consider encrypting the information that is stored in the cookies you use.**
- ☐ **Consider hiring a penetration testing service to assess the security of your public-facing web application(s) at least once a year.**

TRAINING EMPLOYEES

- ☐ **Teach your employees accountability and strategies to minimize human error that could expose customer data. This means advising them to:**
  - Minimize their access to and transmission of customer data to only what is necessary to perform their job functions,
  - Maintain strong security practices on all devices and accounts that deal with customer data by using strong passwords, enabling two-factor authentication, keeping software updated, and not clicking on suspicious links, and
  - Report any potential internal or external security incidents, threats, or mishandling of customer data to your organization's technical personnel and/or higher management.
- ☐ **Ensure your employees understand and have signed documents to adhere to your organization's data protection and security policies.**

NOTIFYING CUSTOMERS

- ☐ **Build an awareness of your organization's regulatory environment when it comes to handling customer data breaches to ensure you are prepared to comply when incidents do occur.**
- ☐ **When your organization becomes aware of an incident of unauthorized access to sensitive customer information, investigate to promptly determine the likelihood that the information has been or will be misused. Follow notification best practices and notify the affected customer(s) as soon as possible with:**
  - A general description of the incident and the information that was breached;
  - A telephone number for further information and assistance;
  - A reminder "to remain vigilant" over the next 12 to 24 months;
  - A recommendation that incidents of suspected identity theft be reported promptly;
  - A general description of the steps taken by the financial institution to protect the information from further unauthorized access or use;
  - Contact information for credit reporting agencies; and
  - Any other information that is required by regulations with which your organization must comply.