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.

CYBERSECURITY FOR SMALLER ORGANIZATIONS

CISO CHECKLIST: PROTECTING CONNECTIONS TO THIRD PARTIES

CHOOSING VENDORS WITH CYBERSECURITY IN MIND

Each time you are evaluating a potential vendor, check off the following questions:

- □ What experience do they have serving clients similar to your organization?
- □ Have they documented their compliance with known cybersecurity standards (such as the NIST Framework or ISO 27001, or can they provide a SOC2 report)?
- □ Which of your data and/or assets will they need to access to perform their services, and are they requesting any apparently unnecessary access?
- □ How do they plan to protect your organization's assets and data that are in their possession?
- □ How do they manage their own third-party cyber risk, and can they provide information about their supply chain security?
- □ What is their plan for disaster recovery and business continuity in case of an incident impacting your organization?
- □ How will they keep your organization updated in terms of communicating trends, threats, and changes within their organization?

IDENTIFYING RISK THROUGH THIRD PARTIES

Perform a third party cyber risk assessment including the following steps:

- □ Create and continuously update a list of all vendor relationships and the assets and data that are exposed in each.
- □ Conduct a review of the data that each vendor or third party has access to, ensuring that each level of access adheres to the principle of "least privilege."
- □ Rank your vendor and third party relationships (low, medium, high) based on the impact that a breach of their systems would have on your organization.
- □ Starting with the highest risk vendors, evaluate each provider's cybersecurity capabilities and compliance with relevant standards.
- □ Develop a plan for regular security evaluation, keeping in mind that you may occasionally want to conduct on-site assessments of vendors with the highest risk and/or greatest access to customer data.

MANAGING THIRD PARTY SECURITY

- □ Perform thorough due-diligence. Establish cybersecurity expectations in all requests for proposals, contracts, business continuity, incident response, and service level agreements with vendors. Agree on responsibilities and liabilities in case of a cyber incident.
- □ Inquire about the cybersecurity practices of financial organizations and other entities with which you transact or share data, keeping in mind that your vendors and third parties should also be following any cybersecurity requirements that your organization must meet.

□ Use established and agreed upon measures to monitor your vendors' compliance with cybersecurity standards.

□ Check with your vendors that handle sensitive data to see if they offer two-factor authentication, encryption, or other security measures for any accounts you have with them.

□ Ensure that all third party software and hardware you install have a security handshake so that booting processes are secured via authentication codes and will not execute if codes are not recognized.

□ If you encounter vendor products that are either counterfeit or do not match specifications, work to negotiate a resolution or else an exit strategy.

□ Annually evaluate vendor contracts and ensure that they continue to meet your strategic direction and regulatory data security requirements. Upon contract termination, include stipulations about getting your assets or data back and verifying that the assets or data are completely erased on the vendor's side, and disable any access to your systems or servers.

SHARING INFORMATION

□ Ensure that you have clear communication channels and points of contact to communicate about security issues with your organization's vendors and counterparts.

□ Check that you have procedures in place to ensure timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector).

□ Track relevant updates about what other organizations are experiencing with their third parties in terms of threats, vulnerabilities, incidents, and responses by becoming part of information-sharing organizations like FS-ISAC and seeking other threat information sources.

CYBERSECURITY FOR SMALLER ORGANIZATIONS

INCIDENT RESPONSE CHECKLIST

PREPARING

□ Work with your organization's senior leadership and other relevant personnel to develop an incident response and business continuity plan based on the most pressing risks that have been identified in your organization's cyber risk assessment.

□ Develop threat scenarios for the kinds of incidents that relate to your organization's highest-priority cyber risks. Focus on building capacity to respond to those scenarios.

□ Identify, record, and make available within your organization a list of points of contact for incident response.

□ Identify and record contact information for relevant local and federal law enforcement agencies and officials.

□ Establish provisions specifying which kinds of incidents must be reported, when they must be reported, and to whom.

□ Establish written guidelines that outline how quickly personnel must respond to an incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident.

□ Inform all employees to contact your technical team—most commonly this will be IT personnel and/or CISO/CIO/other comparable manager—when an incident occurs.

□ Deploy solutions to monitor employee actions and to enable identification of insider threats and incidents.

□ Include business continuity plans to coordinate how your organization will work with suppliers and primary customers during a business emergency, including how you would conduct manual or alternative business operations if required.

□ Include written procedures for emergency system shutdown and restart.

□ Develop and test methods for retrieving and restoring backup data; periodically test backup data to verify its validity.

□ Have established agreements and procedures for conducting business operations in an alternate facility/site.

□ Have in place a clear dissemination channel to all customers.

□ Develop and test methods for retrieving and restoring backup data; periodically test backup data to verify its validity.

□ Have established agreements and procedures for conducting business operations in an alternate facility/site.

□ Have in place a clear dissemination channel to all customers.

EXERCISING

□ Organize small tabletop exercises with all staff or representatives from all levels of staff, including your organization's executives, PR/communications personnel, and legal and compliance teams.

□ Identify and ideally participate in industry-wide tabletop exercises relevant for your organization.

□ Establish a process to ensure lessons learned from exercises are incorporated and addressed in your company's cybersecurity strategy.

RESPONDING

- □ Implement incident response plan actions to minimize the impact on business operations.
- □ Identify impacted/compromised systems and assess the damage.
- □ Reduce damage by removing (disconnecting) affected assets.
- □ Start recording all information as soon as the team suspects that an incident has occurred. Attempt to preserve evidence of the incident while disconnecting/segregating affected identified assets (e.g., collect the system configuration, network, and intrusion detection logs from the affected assets).
- □ Notify appropriate internal parties, third-party vendors, and authorities, and request assistance if necessary.
- □ Initiate customer notification and assistance activities consistent with laws, regulations, and inter-agency guidance.
- □ Use threat sharing platforms such as FS-ISAC or MISP to notify the industry about the threat.
- □ Document all steps that were taken during the incident to review later.

RECOVERING

- □ Restore recovered assets to periodic "recovery points" if available and use backup data to restore systems to last known "good" status.
- □ Create updated "clean" backups from restored assets and ensure all backups of critical assets are stored in a physically and environmentally secured location.
- □ Test and verify that infected systems are fully restored. Confirm that affected systems are functioning normally.

REVIEWING

- □ Conduct a "lessons learned" discussion after the incident occurred—meet with senior staff, trusted advisors, and the computer support vendor(s) to review possible vulnerabilities or recommend new steps to be implemented.
- □ If possible, identify the vulnerabilities (whether in software, hardware, business operations, or personnel behavior) that led to the incident and develop a plan to mitigate them.
- □ Confirm that affected systems are functioning normally.
- □ Develop a plan for monitoring to detect similar or further incidents related to the issues identified.
- □ Share lessons learned and information about the incident on threat sharing platforms such as FS-ISAC.
- □ Integrate lessons learned in your organization's incident response protocols.

CYBERSECURITY FOR SMALLER ORGANIZATIONS

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.

CYBERSECURITY FOR SMALLER ORGANIZATIONS

WORKFORCE DEVELOPMENT CHECKLIST

FUNDAMENTAL APPROACHES TO CYBERSECURITY WORKFORCE DEVELOPMENT

□ **Expand the supply pipeline.**

- Does your organization have relationships with universities and technical colleges?
- Do you offer cybersecurity internships and apprenticeships?

□ **Identify and match existing supply with talent openings.**

- Is your human resources department effectively translating required skills into posted job descriptions?

□ **Retrain existing staff to become part of the cyber workforce.**

- Is your organization leveraging existing talent by shifting resources to its cyber workforce?

□ **Reduce the demand on your cyber workforce through technological innovation.**

- Do you have agreements with third-party service providers to create surge capacity?

□ **Improve retention of the current workforce.**

- Is your organization investing in talented team members?
- Does your organization allow interested individuals to explore careers in cybersecurity?

IDENTIFYING NEEDS

□ **Identify your workload requirements.**

□ Evaluate the complexity of your operations and the speed with which actions need to be executed.

□ Consider surge capacity needs and whether advanced technologies can help reduce attack surface.

□ **Identify your workforce requirements.**

□ Consider the competency, flexibility, and agility of the cybersecurity workforce in your organization.

□ Identify ideal reporting structures and highlight where multi-functionality is preferable.

□ **Define the required knowledge, skills, abilities, and competency of your cybersecurity workforce based on the business functions they support.**

□ **Identify critical gaps in your organization's existing cybersecurity workforce.**

□ Employ existing tools such as the NICE framework to guide internal assessments of roles and responsibilities.

IMPROVING EXTERNAL RECRUITMENT

□ **Strengthen job postings by writing clear, internally consistent job descriptions.**

- □ Use existing tools such as the NICE framework to highlight relevant skill sets.

□ **Gather data on recruitment through the application process.**

- □ Systematize data collection and share throughout the company to prevent silo formation and support talent sourcing and development.
- □ Evaluate recruitment data periodically to identify gaps in outreach.

□ **Rely on multiple indicators to assess candidate potential.**

- □ Consider implementing systematized hiring assessments.
- □ Evaluate relevant degrees, certifications, and work experiences.
- □ Avoid relying on one specific metric when making hiring decisions.

ADVANCING INTERNAL TRAINING AND DEVELOPMENT

□ **Develop career maps that highlight advancement tracks for your cybersecurity workforce.**

□ **Identify pathways within your organization for retraining and repositioning staff into cybersecurity roles.**

- □ Consider potential nontraditional entry points into cybersecurity based on interest and ability.
- □ Expand upskilling and retraining programs and incentivize transitions within your organization.

□ **Encourage internal training and independent learning.**

- □ Open opportunities for continued education and skill certification.

□ **Track data on workforce retention.**

- □ Evaluate retention data periodically to identify whether programs are meeting employee needs.