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.