CISO-LEVEL GUIDE: PROTECTING CONNECTIONS TO THIRD PARTIES

IDENTIFYING RISK THROUGH THIRD PARTIES

- Create and keep an updated list of all vendor relationships and the assets and data exposed in each.
- Review the data that each vendor or third party has access to. Ensure that this 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. Compliance with relevant standards is a good starting point. Develop a plan for regular security evaluation. You may want to occasionally 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 your organization's 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 other third parties such as financial organizations with which you transact or share data. Any cybersecurity requirements to which your organization must adhere should also be followed by your vendors and any other organizations you share data with or expose assets to.
- 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.
- Engage in 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 to enhance your organization's defenses, increase situational awareness, and broaden learning. Being part of information-sharing organizations, for example, the FS-ISAC, will facilitate being up to date.

How to Choose Vendors With Cybersecurity in Mind

Ask the following questions of potential vendors to gauge their cyber preparedness and awareness and consequently the impact they would have on your organization's risk profile:

1. **What experience do they have?** Find out about the vendor's history serving clients. Have they served clients similar to your organization before?
2. **Have they documented their compliance with known cybersecurity standards** such as the NIST Framework or ISO 27001, or can they provide a SOC2 report?
3. **Which of your data and/or assets will they need to access to perform their services?** Are they requesting any apparently unnecessary access?
4. **How do they plan to protect your organization's assets and data that are in their possession?**
5. **How do they manage their own third-party cyber risk?** Can they provide information about their supply chain?
6. **What is their plan for disaster recovery and business continuity** in case of an incident impacting your organization's assets and/or data?
7. **How will they keep your organization updated?** What is their plan for communicating trends, threats, and changes within their organization?

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America