CYBERSECURITY FOR SMALLER FINANCIAL ORGANIZATIONS

BOARD CHECKLIST: CYBERSECURITY LEADERSHIP

FUNDAMENTALS OF CYBER RISK GOVERNANCE

- ☐ As a group, periodically assess whether the board can affirmatively answer the following questions:
  - Has your organization met relevant statutory and regulatory requirements, for example, GDPR?
  - Has your organization quantified its cyber exposures and tested its financial resilience?
  - Does your organization have an improvement plan in place to ensure exposures are within your agreed-upon risk appetite?
  - Does the board regularly discuss concise, clear, and actionable information regarding the organizatoin's cyber resilience supplied by management?
  - Does your organization have incident response plans in place that have been recently dry-run exercised, including at board-level?
  - Are the roles of key people responsible for managing cyber risk clear and aligned with the three lines of defense?
  - Have you obtained independent validation and assurance of your organization's cyber risk posture, for example, via testing, certification, or insurance?
- ☐ If you cannot affirmatively answer one or more of the above, work with your CEO, CISO, relevant organization personnel, and/or external resources to correct the issue.

OVERSIGHT

- ☐ Ensure that the board is aware of its role as the ultimate responsibility-holder for your organization's cyber risk and resilience.
  - ☐ Delegate oversight to a specific board committee if deemed necessary.
- ☐ Assign one corporate officer, usually designated the chief information security officer (CISO), to be accountable for reporting on your organization's capability to manage cyber resilience and progress in implementing cyber resilience goals.
  - ☐ Ensure that this officer has regular board access, sufficient authority, command of the subject matter, experience, and resources to fulfill these duties.
- ☐ Annually define your organization's risk tolerance, ensuring it is consistent with your corporate strategy and risk appetite.
- ☐ Ensure that a formal, independent cyber resilience review of your organization is carried out annually.
- ☐ Work to integrate cyber resilience and risk assessment into your organization's overall business strategy, risk management, budgeting, and resource allocation.
- ☐ Oversee the creation, implementation, testing and ongoing improvement of cyber resilience plans, ensuring they are harmonized across your organization and that your CISO or other accountable officer regularly reports on them to the board.
- ☐ Periodically review your performance of the above and consider seeking independent advice for continuous improvement.

STAYING INFORMED

- ☐ When an individual joins the board, ensure that they have appropriate and up-to-date skills and knowledge to understand and manage the risks posed by cyber threats.
- ☐ Solicit regular advice from management on your organization's current and future risk exposure, relevant regulatory requirements, and industry and societal benchmarks for risk appetite. Plan to engage in:
  - Regular briefings on duties created by new regulations and legislation,
  - Board and executive committee joint planning and visits to best practice peers and leaders in cybersecurity,
  - Security briefings on the threat environment, and
  - Board-level exchanges of information on governance and reporting.
- ☐ Make clear to management that they are accountable for reporting a quantified and understandable assessment of cyber risks, threats, and events as a standing agenda item during board meetings.
- ☐ Regularly check in with management and other relevant personnel about developments related to ongoing systemic challenges such as supply chain vulnerabilities, common dependencies, and the gap in information sharing between boards on cyber risk governance.

SETTING THE TONE

- ☐ Ensure that staff at all levels recognize that they each have important responsibilities to ensure your organization's cyber resilience.
- ☐ Oversee management's role in fostering and maintaining your organization's risk culture. Regularly assess the effectiveness of your organization's risk culture, considering the impact of culture on safety and soundness and making changes where necessary.
- ☐ Make clear that you expect all staff to act with integrity and to promptly escalate observed non-compliance within or outside your organization.

CYBERSECURITY FOR SMALLER FINANCIAL ORGANIZATIONS

CEO CHECKLIST: CYBERSECURITY LEADERSHIP

GOVERNANCE

- ☐ Appoint a Chief Information Security Officer (CISO) if none exists.
- ☐ Establish and maintain an organization-wide cybersecurity policy that is risk-based and informed by international, national, and industry standards and guidelines.
- ☐ Define roles and responsibilities for all personnel involved in cybersecurity. Work with your CISO to identify proper cybersecurity roles and access rights for all levels of staff.
- ☐ Establish or identify clear communication channels between any separate units or personnel that deal with different aspects of cybersecurity.
- ☐ Ensure your CISO has a clear, direct line of communication to relate threats in a timely manner to you and to the board.
- ☐ Maintain a regular invitation for your CISO or other technical personnel to brief senior management.
- ☐ Check that cybersecurity policies, standards, and mechanisms are uniform across the entire organization.

RISK ASSESSMENT AND MANAGEMENT

- ☐ Conduct a cybersecurity risk assessment in collaboration with your CISO or other technical personnel, which should include:
  - Describing your organization's assets and their various levels of technology dependency,
  - Assessing your organization's maturity and the inherent risks associated with its assets' technology dependencies,
  - Determining your organization's desired state of maturity,
  - Understanding where cybersecurity threats sit in your organization's risk priority list,
  - Identifying gaps between your current state of cybersecurity and the desired target state,
  - Implementing plans to attain and sustain maturity,
  - Continuously reevaluating your organization's cybersecurity maturity, risks, and goals, and
  - Considering protective measures such as buying cyber insurance.
- ☐ Analyze and present results to key stakeholders and the board.
- ☐ Plan to oversee any steps to increase cyber preparedness and monitor progress.

ORGANIZATIONAL CULTURE

- ☐ Regularly discuss cyber risk and security at the leadership level.
- ☐ Ensure that cybersecurity training is part of all employee onboarding and have all employees sign documents agreeing to adhere to the organization's cybersecurity policies.
- ☐ Establish recurring cybersecurity training for all staff.
- ☐ Ensure that cybersecurity is always considered when the organization evaluates potential vendors and shares data with third parties.
- ☐ Institute an annual review of the organization's cybersecurity policies.
- ☐ Encourage technical personnel to engage in voluntary information sharing about cybersecurity threats and incidents.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

CYBERSECURITY FOR SMALLER FINANCIAL ORGANIZATIONS

CISO CHECKLIST: PROTECTING YOUR ORGANIZATION

DEVELOPING A RISK-BASED INFORMATION SECURITY PROGRAM

- ☐ Identify and list all the types of information your business stores and uses (e.g. customer names and email).
- ☐ Ask and record answers for each information type:
  - What would happen if this information was made public?
  - What would happen to my business if this information was incorrect?
  - What would happen to my business if I/my customers couldn't access this information?
- ☐ Record what technology comes into contact with the information you have identified. This can include hardware (e.g. computers) and software applications (e.g. browser email).
  - Where applicable, include technologies outside of your business (e.g. "the cloud") and any protection technologies you have in place such as firewalls.
  - Include the make, model, serial numbers, and other identifiers.
  - Track where each product is located. For software, identify what machine(s) the software has been loaded onto.
- ☐ Regularly review information from your national CERT, FS-ISAC, your local InfraGard chapter, and others about what threats and vulnerabilities the financial sector may face and estimate the likelihood you will be affected.
- ☐ Conduct a vulnerability scan or analysis at least once a year.
- ☐ Create a cybersecurity policy for your organization.
- ☐ Train all employees on the details of the policy and have them sign documents acknowledging their role in continuously upholding your organization's cybersecurity by adhering to the policy.

PREVENTING MALWARE DAMAGE

- ☐ Activate your firewall and set access control lists (ACLs. Restrict access by using a whitelisting setting.
- ☐ Use antivirus software and antispyware on all computers and laptops.
- ☐ Apply the latest software updates provided by manufacturers and vendors. 'Automatically update' where available.
- ☐ Restrict installation of new programs to IT staff with admin rights.
- ☐ Maintain and monitor activity logs generated by protection / detection hardware or software. Protect logs with password protection and encryption.
- ☐ Ensure all host clocks are synchronized.
- ☐ Control access to removable media such as SD cards and USB sticks. Encourage staff to transfer files via email or cloud storage instead. Educate staff on the risks of using USBs from external sources or handing over their USBs to others.
- ☐ Set up email security and spam filters on your email services.
- ☐ Protect all pages on your public-facing websites with encryption and other available tools.
- ☐ Consider hiring a penetration testing service to assess the security your organization's assets and systems.

TRAINING EMPLOYEES

- ☐ Plan to run mandatory cybersecurity trainings during all new employee onboarding and at regular intervals for current employees at least once annually. Require employees to:
  - Use strong passwords on all professional devices and accounts and encourage them to do the same for personal devices and to use a password manager,
  - Keep all operating systems, software, and applications up to date across all devices,
  - Use two-factor authentication on all accounts,
  - Keep account details and access cards secure and lock devices when unattended,
  - Refrain from sharing account details or other sensitive data via unencrypted email or other open communications,
  - Avoid immediately opening attachments or clicking links in unsolicited or suspicious emails,
  - Verify the validity of a suspicious looking email or a pop-up box before providing personal information, and pay close attention to the email address, and
  - Report any potential internal or external security incidents, threats, or mishandling of data or devices to your organization's technical personnel and/or higher management.
- ☐ Plan and carry out regular tests of employee awareness through simulations such as sending phishing-style emails from fake accounts. Assess any employee failures and use them as opportunities for learning and improvement.

PROTECTING YOUR DATA

- ☐ Take regular backups of your important data (e.g. documents, emails, calendars) and test that they can be restored. Consider backing up to the cloud.
- ☐ Ensure the device containing your backup is not permanently connected to the device holding the original copy, neither physically nor over a local network.
- ☐ Install surge protectors, use generators, and ensure all of your computers and critical network devices are plugged into uninterruptible power supplies.
- ☐ Use a mobile device management (MDM) solution.

KEEPING YOUR DEVICES SAFE

- ☐ Switch on PIN or password protection for mobile devices. Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.
- ☐ Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.
- ☐ When sending sensitive data, don't connect to public Wi-Fi hotspots – use cellular connections (including tethering and wireless dongles) or use VPNs.
- ☐ Replace devices that are no longer supported by manufacturers with up-to-date alternatives.
- ☐ Set reporting procedures for lost or stolen equipment.

USING PASSWORDS

- ☐ Make sure all computers use encryption products that require a password to boot. Switch on password or PIN protection for mobile devices.
- ☐ Use strong passwords, avoiding predictable passwords (like passw0rd) and personal identifiers (such as family and pet names). Instruct all employees to do the same.
- ☐ Use two-factor authentication (2FA) wherever possible.

- ☐ Change the manufacturer-issued default passwords on all devices, including network and IoT devices, before they are distributed to staff.

- ☐ Ensure staff can reset their own passwords easily. You may also want to require staff to change their password at regular intervals (e.g., quarterly, half yearly, or annually).
- ☐ Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

CONTROLLING PERMISSIONS

- ☐ Ensure that all personnel have uniquely identifiable accounts that are authenticated each time they access your systems.
- ☐ Only give administrative privileges to trusted IT staff and key personnel and revoke administrator privileges on workstations for standard users.
- ☐ Only give employees access to the specific data systems that they need for their jobs and ensure they cannot install any software without permission.
- ☐ Create user accounts for each employee on your organization's computers.

SECURING YOUR WI-FI

- ☐ Make sure your workplace Wi-Fi is secure and encrypted with WPA2. Routers often come with encryption turned off, so make sure to turn it on. Password protect access to the router, and make sure that the password is updated from the pre-set default. Turn off any "remote management" features.
- ☐ Set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID).
- ☐ Limit access to your Wi-Fi network by only allowing devices with certain media access control addresses. If customers need Wi-Fi, set up a separate public network.
- ☐ Enable Dynamic Host Configuration Protocol (DHCP) logging on your networking devices to allow for easy tracking of all devices that have been on your network.
- ☐ Log out as administrator after you have set up the router.
- ☐ Keep your router's software up to date. Register your router with the manufacturer and sign up to get updates.

AVOIDING PHISHING ATTACKS

- ☐ Ensure staff don't browse the web or check emails on servers or from an account with Administrator privileges.
- ☐ Set up web and email filters. Consider blocking employees from visiting websites commonly associated with cybersecurity threats.
- ☐ Teach employees to check for obvious signs of phishing, like poor spelling and grammar, or low-quality versions of recognizable logos. Does the sender's email address look legitimate?
- ☐ Scan for malware and change passwords as soon as possible if you suspect an attack has occurred. Don't punish staff if they become the victim of a phishing attack (it discourages people from reporting in the future).

CYBERSECURITY FOR SMALLER FINANCIAL 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 FINANCIAL 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 disenable 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 FINANCIAL 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.