Cybersecurity Capacity-building
Tool Box for Financial Organizations

CISO-Level Guide: Protecting Your Organization

Developing a Risk-Based Information Security Program

1. Identify the types of information your business stores and uses

⇒ List all of the types of information your business stores or uses (e.g. customer names and email).

2. Define the value of your information

⇒ Ask key questions for each information type:

- What would happen if this information was made public?
- What would happen to my business if this information was incorrect e.g., the integrity of the data had been manipulated?
- What would happen to my business if I/my customers couldn't access this information?

3. Develop an inventory

⇒ Identify 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). 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.

⇒ Where applicable, include technologies outside of your business (e.g. "the cloud") and any protection technologies you have in place such as firewalls.

4. Understand your threats and vulnerabilities

⇒ Regularly review what threats and vulnerabilities the financial sector may face and estimate the likelihood that you will be affected. (Information can be found via your national CERT, FS-ISAC, and other local and regional groups.)

⇒ Conduct a vulnerability scan or analysis at least once a year.

5. Create a cybersecurity policy

⇒ Work with your organization's senior management to establish and maintain a cybersecurity strategy that is tailored to the above risks and informed by international, national, and industry standards and guidelines. Guidelines such as the NIST Framework, the FFIEC's Cybersecurity Assessment Tool, and ISO 27001 provide foundations for such policies.

⇒ 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) to create a buffer zone between your network and the Internet. Restrict access by using a whitelisting setting, not blacklisting certain IP addresses or services.

⇒ Use antivirus software and antispyware on all computers and laptops.

⇒ Patch all software and firmware by promptly applying 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.

⇒ Keep all host clocks synchronized. If your organization's devices have inconsistent clock settings, event correlation will be much more difficult when incidents occur.

⇒ 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 own 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 of your assets and systems.

Training Employees

⇒ Run mandatory cybersecurity trainings during new employee onboarding and at regular intervals for all 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.

⇒ Regularly test employee awareness through simulated issues such as by sending phishing-style emails from fake accounts. Use any failures as opportunities for learning rather than punishment.

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 and 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.
⇒ Control physical access to your computers and create user accounts for each employee.

Securing Your Wi-Fi Networks and Devices

⇒ 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. Hear about updates by registering your router with the manufacturer and signing 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 (e.g., poor spelling, grammar, or low-quality versions of 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).

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

INTERNATIONAL MONETARY FUND

SWIFT INSTITUTE

FS-ISAC

Standard Chartered

CYBER READINESS INSTITUTE

GLOBAL CYBER ALLIANCE