JULY 2019

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

SWIFT INSTITUTE

FS-ISAC

Standard Chartered

CYBER READINESS INSTITUTE

GLOBAL CYBER ALLIANCE

Capacity-Building Tool Box for Cybersecurity and Financial Organizations

Tim Maurer and Kathryn Taylor

Capacity-Building Tool Box for Cybersecurity and Financial Organizations

Tim Maurer and Kathryn Taylor

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

CONTENTS CONT.

CONTENTS

About the Authors

Tim Maurer is co-director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace and author of the book *Cyber Mercenaries: The State, Hackers, and Power* published by Cambridge University Press in 2018. He is an internationally recognized expert on cybersecurity and geopolitics in the digital age and leads Carnegie's FinCyber project dedicated to cybersecurity and the financial system.

Kathryn Taylor is a nonresident expert with the Cyber Policy Initiative at the Carnegie Endowment for International Peace, where she focuses on capacity-building measures to improve cyber resiliency in the financial sector. She is a graduate of Emory University with degrees in computer science and international studies.

Acknowledgments

A priority throughout this project was the integration of an iterative feedback loop. We are therefore particularly grateful to the several dozen experts in central banks, ministries of finance, cybersecurity agencies, international bodies and industry that provided input during the early stages as well as feedback on advanced drafts of this work, namely Anil Kuril, Union Bank of India; Asadullah Fayzi, Afghanistan International Bank; Boston Banda, Reserve Bank of Malawi; Curtis Dukes and Tony Sager, CIS (Center for Internet Security); Juan Carlos Crisanto, Denise Garcia Ocampo, and Johannes Ehrentraud at the Bank for International Settlements; Petra Hielkema and Raymond Kleijmeer, De Nederlandsche Bank; Phil Venables, Aimée Larsen Kirkpatrick and Alejandro Fernández-Cernuda, Global Cyber Alliance, Shafique Ibrahim, Al Fardan Group; Silvia Baur-Yazbeck and David Medine, Consultative Group to Assist the Poor; the experts at the FS-ISAC; the experts at the UK Financial Conduct Authority; the experts at the IMF; and the experts at the SWIFT Institute. Several experts from other institutions who shared feedback preferred to remain anonymous.

Official Partners

Glossary

CPMI-IOSCO	Committee on Payments and Market Infrastructures – International Organization of Securities Commissions
EU	European Union
FCC	U.S. Federal Communications Commission
FFIEC	U.S. Federal Financial Institutions Examination Council
FSB	Financial Stability Board
FS-ISAC	Financial Services – Information Sharing and Analysis Center
FTC	U.S. Federal Trade Commission
GDPR	EU General Data Protection Regulation
IMF	International Monetary Fund
NCSC	UK National Cyber Security Centre
NIS Directive	EU Directive on the security of network and information systems
NIST	U.S. National Institute of Standards and Technology
SWIFT	Society for Worldwide Interbank Financial Telecommunication

Executive Summary

The global financial system is facing growing cyber threats and increased risk. In 2017, the G20 Finance Ministers and Central Bank Governors warned that "[t]he malicious use of Information and Communication Technologies could … undermine security and confidence and endanger financial stability."[1] These concerns have led to a flurry of regulatory and policy activity in recent years at both the international and national levels from the Financial Stability Board to the IMF, CPMI, and IOSCO as well as the EU, India, China, Singapore, and the U.S. and, on the industry side, from SWIFT's Customer Security Program to FS-ISAC and Sheltered Harbor.[2]

There is a clear need for financial institutions to be vigilant to avoid potentially large losses or reputational damage. In fact, the year 2016 was a wake-up call for the financial sector when malicious hackers tried to steal $1 billion from the Bank of Bangladesh. They ultimately succeeded at stealing $81 million by sending fraudulent instructions and exploiting multiple systemic vulnerabilities.[3] The incident's headlines became an urgent warning of systemic risk, and financial organizations worldwide sprang into action.

Less cyber-mature and smaller financial organizations deserve special attention but have been neglected so far. Many of the latter are particularly vulnerable, constrained by fewer resources, smaller staff, and often less experience. In 2018, 58 percent of overall victims of cyberattacks were small businesses.[4] Some reports suggest credit unions and banks with less than $35 million in assets account for the majority of hacking and malware breaches in the financial sector.[5] Moreover, incidents dating back to 2016 suggest that some threat actors specifically target financial organizations in the Global South and low-income countries.[6]

Minimizing overall cyber risk to the financial sector depends upon the protection and participation of smaller organizations such as credit unions, savings banks, building societies, trust companies, account servicers, and even end customers. A system's cybersecurity is only as strong as its weakest links. In addition, smaller financial organizations are more likely to serve more vulnerable, low-income communities and thus are often key providers of financial inclusion programs. **Cyber incidents involving smaller financial organizations could therefore hamper efforts to enhance financial inclusion**, undermine consumer trust, and curb the use of needed financial resources.

To enhance the cybersecurity of less cyber-mature and smaller financial institutions, **this project offers a package of easy-to-use, action-oriented, practical one-page guides detailing how institutions can enhance their own security as well as that of their customers and third parties**; information about cyber incidents; and a comprehensive, supplementary report.

Project's Approach and Methodology

Governments, businesses, and international bodies have been increasing their efforts to increase the cybersecurity of financial institutions. For example, starting in 2016, central banks around the world established new units dedicated to cybersecurity, which simply did not exist before.[7] Even the G7 countries decided to launch a new process as a catalyst to tackle this growing risk.[8] Unsurprisingly, these efforts have been uneven and remain nascent. Therefore, capacity-building efforts focusing on low-income countries, less cyber-mature and smaller organizations across the world remain in their infancy. Guidance on basic cyber hygiene and best practices that form a baseline for cybersecurity generally have yet to reach these organizations.

Theory of Change: If proper information and quality security practices are promulgated in digestible, actionable forms – as this project seeks to achieve – financial organizations can quickly improve their basic cyber hygiene. Smaller financial institutions, in particularly, can use their size to their advantage in terms of ease and speed of adoption of cybersecurity measures. With fewer staff members and less institutional red tape, they can approve, implement, and streamline policies and practices with agility. Along the way, crucial support and guidance can be found through collaboration and exchanges with industry partners, regulators, and supervisors, and public and private cybersecurity organizations.

Our Tool Box Contains:

- Board-Level Guide: Cybersecurity Leadership
- CEO-Level Guide: Cybersecurity Leadership
- CISO-Level Guides:
  - Protecting Your Organization
  - Protecting Your Customers
  - Protecting Connections to Third Parties
- Incident Response Guide

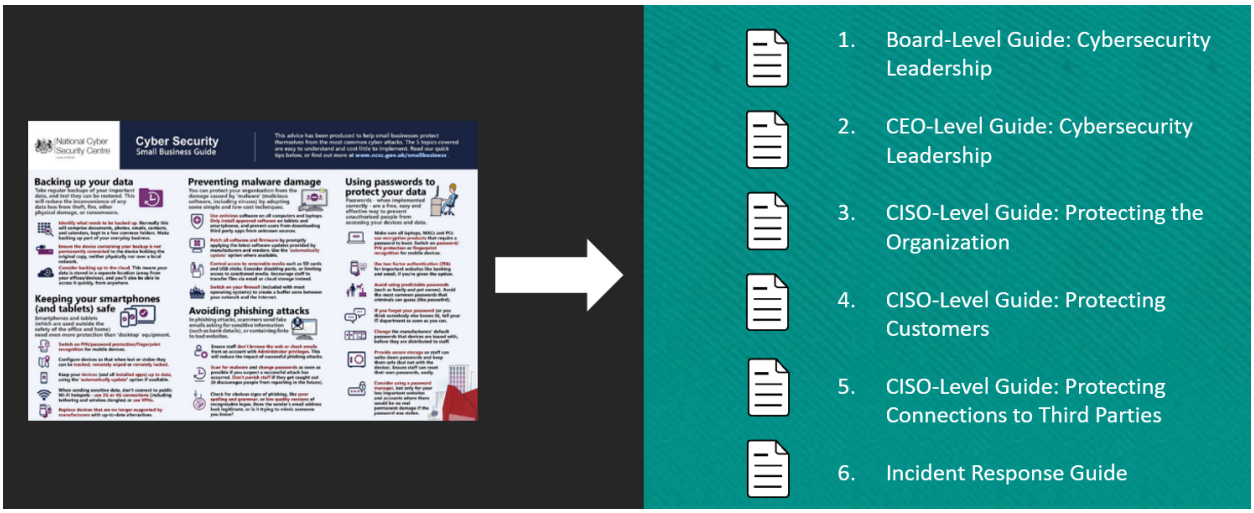
Building on Existing Best Practices: This report presents a new tailored approach with best practices that have been carefully curated to meet the most pressing cybersecurity needs of less cyber-mature and smaller financial organizations while remaining achievable within their resources and capabilities. What is contained herein is not a new invention, though. Seeking to build on existing best practices, we began the development process with substantial desk research into the two areas of existing guidance: first, cybersecurity guidance for small businesses generally (not focused on financial institutions) and, second, cybersecurity guidance for financial institutions (usually not focused on small entities). Together, they provide highly valuable frameworks with risk-based approaches, recommendations for widely achievable cyber hygiene improvements, and measures tailored to small businesses and specific sectors.[9]

Multiple Feedback Loops: Upon reviewing existing material, we shared drafts with experts from a variety of national and international institutions to gauge the relative utility and practicability of the various strategies and measures. Engaging with experts from several central banks and commercial banks as well as other institutions including the IMF, FS-ISAC, and SWIFT enabled us to synthesize

the patchwork of existing guidance into a package of targeted, high-yield recommendations for less cyber-mature and smaller financial organizations.

Key Findings: Taking inspiration from a guide for small businesses created by the UK's NCSC (see Appendix), we have presented the best practices as groups of tangible activities aimed at building capacity and protecting against specific threats.[10] Yet, as this research progressed, it became clear that effective cybersecurity guidance must inform behavior not only at the technical level but at many other decision points, from executive strategy to employee awareness to third party interactions. This led us to develop mutually reinforcing sets of best practices for CEOs and chief information security officers (CISOs) that, altogether, cover governance, IT measures, employee training and behavior, customer data security, vendor management, and organization-wide incident response.

Figure 1: Goal - Developing Practical and Actionable One-Page Guides with Best Practices



What's in the Package: Our series of six one-page guides starts at the board and executive levels to ensure comprehensive risk management, organized governance, and continuous organizational thinking on cybersecurity. From there, it outlines practical measures for CISOs and other personnel to follow to protect critical assets, customers, and connections and to handle incident response. Many of the measures are organization-wide and actionable on an individual level and as such can be made part of employee training and general cybersecurity culture.

An additional resource worth highlighting is the *GCA Cybersecurity Toolkit for Small Business* published by the Global Cyber Alliance in the spring of 2019. This Toolkit offers additional resources complementing the guides and are therefore specifically referenced in the footnotes of this report as well as in hyperlinks embedded in the one-page guides and checklists.

Living Documents: These guides, the report, and the best practices detailed therein must be viewed as living documents and regularly reviewed and updated. The technology continues to evolve and so

must these guides when necessary. Any users of this document should feel free to expand, revise, discuss, and share the recommendations to ensure that they continue to meet their needs in the face of new information and challenges.

Dissemination: A final and crucial consideration is to ensure that these recommendations reach their intended audience of less cyber-mature and smaller financial organizations across the world. For this reason, the guides are now available in seven languages: English, French, Spanish, Portuguese, Arabic, Dutch, and Russian. In addition, based on engagements that have developed throughout this project, we will leverage existing networks of industry groups, governments, and other organizations to make this work as widely publicly available as possible, especially in developing areas.

The following sections briefly describe the guidance put forth in this report.

We welcome any additional support to help disseminate these resources and to help maximize their impact. Also, if you would like to translate the material into an additional language, please do not hesitate to contact us.

Contact details: Tim Maurer tmaurer@ceip.org

Tool Box: Overview

Guidance for Boards and CEOs: Cybersecurity Leadership

An organization's cybersecurity begins and ends with its highest level of management. When a cyber incident occurs – whether money is lost, data is compromised, consumer trust is damaged, or something else happens – the CEO and board are on the front lines dealing with the fallout, both publicly and privately. As such, executives must be involved in developing awareness of their organizations' cyber risk, setting organizational priorities and policies to deal with that risk, and acting as the head of their organization's body of cybersecurity personnel, in particular by having clear and regular communication with technical staff such as their CISO. They also set the tone for the organization writ large and can ensure that the mindset of all employees is focused on identifying and mitigating potential risks including through continuous education and training.

ONE-PAGER #1: Board-Level Guide

The board of directors finds itself at the top of its organization's pyramid of accountability for cyber preparedness and response. Its level of savviness, engagement, and visible leadership are therefore critical to the organization's cyber resilience. This section offers recommendations for boards to take an active role in their organizations' cybersecurity, to gain the up-to-date information they need to do so, and to self-reflect on their leadership:

- *Fundamentals of Cyber Risk Governance* – Providing a list of questions from a report by TheCityUK and Marsh for boards to ask themselves to gauge whether they are meeting essential cybersecurity baselines.

- *Oversight* – Outlining the core leadership functions boards must undertake to effectively govern their organizations' cybersecurity policies and practices.

- *Staying Informed* – Advising boards on how they can ensure individual members and the group as a whole are appropriately knowledgeable about both internal and external cybersecurity trends and challenges.

- *Setting the Tone* – Helping boards understand what it means to lead their organizations' cybersecurity by example, including promoting appropriate risk culture and setting staff expectations.

ONE-PAGER #2: CEO-Level Guide

CEOs play a crucial leadership role when it comes to cybersecurity, simultaneously advising the board and external stakeholders and managing internal personnel and policies. To navigate these dual skillsets and responsibilities, this section offers recommendations for CEOs in the following categories:

- *Governance* – Positioning executives as the leaders of their organizations' cybersecurity by advising them to appoint and articulate roles and responsibilities for cybersecurity staff and to direct efforts to establish organization-wide cybersecurity policies and practices applicable to every member of staff.

- *Risk Assessment and Management* – Directing executives to call for and oversee cyber risk assessment, to digest the results and operationalize them in organizational decision-making, and to ensure ongoing monitoring of cyber risk.

- *Organizational Culture* – Advising executives to include cybersecurity considerations in overall organizational thinking and decision-making and to foster an organization-wide culture of cybersecurity by instituting regular trainings and reviews and making cybersecurity a normal part of communication at all levels.

Guidance for CISOs and Other Personnel: Technical Improvements

At first glance, it may appear that a CISO should only focus on protecting his/her financial institution itself. However, an important lesson learned in recent years has been that a CISO must ensure cybersecurity across the institution's ecosystem and therefore focus not only on (a) the institution itself but also (b) its customers and (c) its third parties.

The remainder of the recommendations in this report therefore outlines best practices for CISOs or other technical personnel to protect their organization, as well as essential cyber hygiene practices that all staff and customers should follow. These tips have been extracted from existing cybersecurity guidance – for the financial sector, for small businesses, and for others more generally – and adapted to be as practical and valuable as possible for less cyber-mature and smaller financial organizations specifically. They are broken down into categories covering the key areas for cybersecurity consideration and protection in the financial sector.

ONE-PAGER #3: CISO-Level Guide: Protecting the Organization

These recommendations are the core building blocks of cybersecurity for organizations and individual employees – practices to secure networks, monitor accounts and activity, protect data, and prevent attacks.

This section begins with foundational guidance for CISOs or equivalent technical personnel to build a risk-based information security program for their organization if they have not yet established one. This information can also be used to review an existing program for all necessary components.

Next, the organization-level guidance identifies important categories of best practices to improve cybersecurity, then describes numerous action steps for each. The categories are:

- *Preventing Malware Damage* – Describing essential cybersecurity practices that CISOs should engage in to secure their organizations' systems such as using firewalls, antivirus software, pen-testing, red-teaming, and physical security measures.
- *Training Employees* – Advising CISOs to make regular, comprehensive staff cybersecurity education a key priority.
- *Protecting Data* – Advising CISOs to keep updated and segmented backups and to take other data protection measures.
- *Securing Devices* – Advising CISOs on how to configure, secure, and handle the life cycle of their organizations' computers, laptops, mobile phones, and other devices.

- *Using Passwords* – Detailing how CISOs should set up password use across their organization and advise employees on how to use secure authentication.

- *Controlling Permissions* – Advising CISOs on how to manage administrative and general employee privileges on their organizations' systems and data.

- *Securing Wi-Fi* – Advising CISOs on how to securely configure their organizations' wireless Internet networks.

- *Avoiding Phishing Attacks* – Identifying the most common indicators of phishing, advising CISOs on preventive steps to take, and advising all employees to stay alert.

ONE-PAGER #4: CISO-Level Guide: Protecting Customers

Customer data is one of the most crucial assets for which financial institutions are responsible. Alongside monetary gain, stealing information about customers' identities, financial accounts, and other personal details is a top motivator for cyber criminals to target financial institutions. When such data is breached, it can harm customers through fraud, theft, and privacy violation.

Banks and other organizations in the financial ecosystem are not just keepers and movers of money but also data stewards and as such must make customer information security a key priority and core competency. This report recommends improving customer security in the following areas:

- *Administering Accounts* – Advising CISOs on how to create and manage customer accounts so that a high level of security is offered by default.

- *Protecting Data* – Advising CISOs to securely handle and store customer information with strong data policies and measures such as encryption.

- *Securing Public Web Applications* – Providing steps for CISOs to take to secure all public-facing channels with which customers may interact and provide data.

- *Training Employees* – Advising CISOs to train employees to handle customer data carefully and responsibly.

- *Notifying Customers* – Describing how CISOs should handle customer notification as part of incident response.

Securing the "long tail" in the financial sector reaches beyond organization-level practices all the way down to the security practices of individual employees and customers. No matter how robust a bank's cybersecurity practices, compromises may still occur if these individuals fail to follow cyber

hygiene practices and unwittingly surrender account credentials or other sensitive data to cyber criminals.

In light of this, in addition to the above organization-level best practices for protecting customer data, this section recommends tips that organizations should give to customers and use to train employees so they can improve their cyber hygiene, protect sensitive data, and avoid falling victim to common attacks such as phishing.

ONE-PAGER #5: CISO-Level Guide: Protecting Connections to Third Parties

A key characteristic of financial organizations is their interconnectivity. The financial system works through transactions and flows of financial and personal data among a network of connected institutions. Further, financial organizations depend on vendors and third-party technologies to deliver their services in an increasingly digital world. Such pervasive dependency opens sensitive new cyber threat vectors that often prove difficult to identify and secure.

Setting and maintaining an organizational standard of cybersecurity cannot succeed if sensitive data or other assets are exposed to third parties that do not adhere to the same level of security. A good start is to develop awareness across financial organizations that their cyber risk assessment and management must always consider their relationships to vendors and third parties and that their contracting and acquisition processes must always consider cybersecurity. To guide this process, this section makes recommendations in the following categories:

- *Choosing Vendors* – Providing CISOs with a list of questions to use to evaluate potential vendors according to their data and cybersecurity practices.
- *Identifying Risk Through Third Parties* – Advising CISOs to maintain up-to-date understanding of their exposure to risk through their third-party relationships.
- *Managing Third Party Security* – Advising CISOs on how to approach cybersecurity as part of service level agreements, technology acquisitions, and other third party relationships, ensuring responsibilities and liabilities are clearly defined.
- *Sharing Information* – Encouraging CISOs to both share and solicit information about the security of their vendor and third party ecosystems.

ONE-PAGER #6: Incident Response Guide

An organization's cybersecurity is tested when incidents actually occur and their preparation must turn into action. Studies show that many firms do not invest sufficiently in response and recovery. Organizations should be prepared that an incident will occur eventually and need to have a plan for response and recovery. Unfortunately, the question is not one of "if" but of "when" such an incident will occur. Having holistic, well-documented incident response plans in place is therefore so crucial to cybersecurity in practice that it merits its own section in this report. It is helpful to understand incident response through the pillars of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover (see Appendix). These pillars describe the lifecycle of incident response and have informed the organization of best practices in this section, which focus on:

- *Preparing* – Providing recommendations for CISOs to develop an incident response plan that will allow their organization to respond to and recover from cyber incidents.
- *Exercising* – Advising organizations to actively prepare and improve incident response by organizing and/or participating in practice exercises.
- *Responding* – Focusing specifically on the crucial steps that must be taken to deal swiftly and responsibly with cyber incidents, from executing damage control to communicating to recording information.
- *Recovering* – Advising CISOs on how to restore systems using backups.
- *Reviewing* – Highlighting that incident response is an iterative process in which each occurrence should be carefully reviewed so that it can be an opportunity to improve cybersecurity procedures and awareness.

Supplementary Report Overview

The supplementary comprehensive report consists of five chapters each beginning with brief guides outlining cybersecurity best practices for less cyber-mature and smaller financial organizations in the categories described above. Following each guide are descriptions, elaborations, and resources to clarify concepts that are mentioned in the guides and to provide information to ease implementation. Each recommendation is heavily footnoted for the purpose of directly linking to additional processes that cannot be fully described here. Many references are made to an organization's CISO and their responsibilities – however, the guides were developed with an understanding that not all organizations may have such an officer and as such contain measures (and implementation details and tips) to allow other IT or operational personnel to carry out those responsibilities.

Board-Level Guide: Cybersecurity Leadership

Fundamentals of Cyber Risk Governance

Confirm that you can affirmatively answer the following questions:

1. Has your organization **met relevant statutory and regulatory requirements**?

2. Has your organization **quantified its cyber exposures and tested its financial resilience**?

3. Does your organization have an **improvement plan** in place to ensure exposures are within your agreed-upon risk appetite?

4. Does the board regularly **discuss concise, clear, and actionable information regarding the organization's cyber resilience supplied by management**?

5. Does your organization have **incident response plans in place that have been recently dry-run exercised**, including at board-level?

6. Are the **roles of key people responsible for managing cyber risk** clear and aligned with the three lines of defense?

7. Have you obtained **independent validation and assurance** of your organization's cyber risk posture?

Oversight

As the highest level of your organization's leadership, the board assumes ultimate accountability for governing cyber risk and therefore must oversee the organization's strategy, policies, and activities in this area. Specifically, the board should:

⇒ Take ultimate responsibility for oversight of cyber risk and resilience, whether as the full board or through delegation of oversight to a specific board committee.
⇒ Assign one corporate officer, usually the 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; ensure consistency with your corporate strategy and risk appetite.
⇒ Ensure that a formal, independent cyber resilience review of your organization is carried out annually.
⇒ Oversee the creation, implementation, testing, and ongoing improvement of cyber resilience plans, ensuring aligned across your organization and that your CISO or other accountable officer regularly reports on them to the board.
⇒ Integrate cyber resilience and risk assessment into your organization's overall business strategy, risk management, budgeting, and resource allocation, with the goal of fully integrating cyber risk into overall operational risk.
⇒ Periodically review your performance of the above and consider independent advice for continuous improvement.

Staying Informed

The board's effective cyber risk oversight depends on members' command of the subject and up to date information.

⇒ Ensure that all individuals joining the board 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. Further, engage in regular briefings on latest developments with respect to the threat landscape and regulatory environment, joint planning and visits to best practice peers and leaders in cybersecurity, and board-level exchanges on governance and reporting.
⇒ Hold management accountable for reporting a quantified and understandable assessment of cyber risks, threats, and events as a standing agenda item during board meetings.
⇒ Maintain awareness of 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

Alongside senior management, the board must set and exemplify your organization's core values, risk culture, and expectations with regard to cyber resilience.

⇒ Promote a culture in which staff at all levels recognize their important responsibilities in ensuring your organization's cyber resilience. Lead by example.
⇒ Oversee management's role in fostering and maintaining your organization's risk culture. Promote, monitor, and assess the 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.

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

CEO-Level Guide: Cybersecurity Leadership

Governance

Your organization's cybersecurity starts and ends at the highest level of management. The CEO, together with the board, must maintain understanding of the risks and assume ultimate accountability and responsibility for the organization's cybersecurity activities and personnel. You should:

⇒ Hire a chief information security officer (CISO) if none exists or, if resources are too limited, appoint somebody within your organization to fulfill the function of a CISO.
⇒ Work with the CISO or other technical personnel to establish and maintain a cybersecurity strategy and framework tailored to the organization's specific cyber risks using international, national, and industry standards and guidelines.
⇒ Articulate clear roles and responsibilities for personnel implementing and managing the organization's cybersecurity.

- Work with the CISO to identify proper cybersecurity roles and access rights for all levels of staff.
- Oversee communication and collaboration to ensure that cybersecurity management is holistic especially if cybersecurity responsibilities are shared by multiple personnel or divisions within the organization (such as having separate information security, risk, and technology verticals).

⇒ Ensure that the CISO has a clear, direct line of communication to relate threats in a timely manner to you and to the board.
⇒ Invite the CISO or other technical personnel to routinely brief senior management.
⇒ Ensure that the organization's security policies, standards, enforcement mechanisms, and procedures are uniform across all teams and lines of business.

Risk Assessment and Management

Ensuring strong cybersecurity awareness and preparedness depends on continuous, risk-based analysis. To improve your organization's cybersecurity:

⇒ Establish cybersecurity risk assessment and management as a priority within your organization's broader risk management and governance processes. Work with your CISO or other technical personnel on a plan to conduct a risk assessment that involves:

- 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 using third party penetration-testing or red-teaming,
- Considering protective measures such as buying cyber insurance.

⇒ Lead employee efforts during the risk assessment process to facilitate timely responses from across the institution.
⇒ Analyze and present the results of the risk assessment for executive oversight, including key stakeholders and the board.
⇒ Oversee any changes to maintain or increase your organization's desired cybersecurity preparedness, ensuring that any steps taken to improve cybersecurity are proportionate to risks and affordable for your organization.
⇒ Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving cyber risk.

Organizational Culture

Your organization's cybersecurity is not a one-time process or the job of a few employees; it is a factor to consider in all business decisions and operations and a practice that must be maintained by all employees. To encourage continuous, holistic cybersecurity within your organization:

⇒ Begin cybersecurity discussions with the leadership team and communicate regularly with the personnel accountable for managing cyber risks.
⇒ Make cybersecurity training a part of all employee onboarding, ensuring that all staff are up to date on – and have signed documents agreeing to adhere to – your organization's cybersecurity policies and that your IT department or other technical personnel have briefed them on best practices.
⇒ Institute recurring cybersecurity training for all staff with regard to their short- and long-term security responsibilities.
⇒ Ensure that cybersecurity is always considered when your organization evaluates potential vendors and shares data with third parties.
⇒ Annually review your organization's cybersecurity policies.
⇒ Encourage voluntary information sharing about cybersecurity threats and incidents within your organization and with trusted counterparts.

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

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
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE

CISO-Level Guide: Protecting Your Customers

Individual Advice for Customers and Employees to Protect Financial Data

Advise your employees and your customers to follow the below cybersecurity guidelines in their personal behavior to increase their preparedness and protect their financial data against cyber threats.

1. Implement basic cyber hygiene practices across your devices.
⇒ 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 your 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.

2. 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. Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky.

3. Resist phishing.
⇒ 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, 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 have 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, ideally require, two-factor authentication for customers to log 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 which 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 across all employees, 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) to prevent cross-site scripting attacks, clickjacking, and other code injection.
⇒ Enable public key pinning on your website(s) to prevent man in the middle attacks.
⇒ Ensure that your public-facing web application(s) never use cookies to store highly sensitive or critical customer information (such as passwords), follow conservative expiration dates for cookies (sooner rather than later), and consider encrypting the information 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 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 so that they do not violate them, so they are fluent when dealing with customers, and so they do not communicate with customers in an unprotected manner.

Notifying Customers

⇒ Understand 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) accordingly 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.

CISO-Level Guide: Protecting Connections to Third Parties

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 beåfore?
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?

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 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.
⇒ 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.

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

Incident Response Guide

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.

Exercising

⇒ Organize small tabletop exercises with all staff or representatives from all levels of staff including 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 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 including with respect to reputational damage.

⇒ 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 asset 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.

⇒ 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.

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

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.

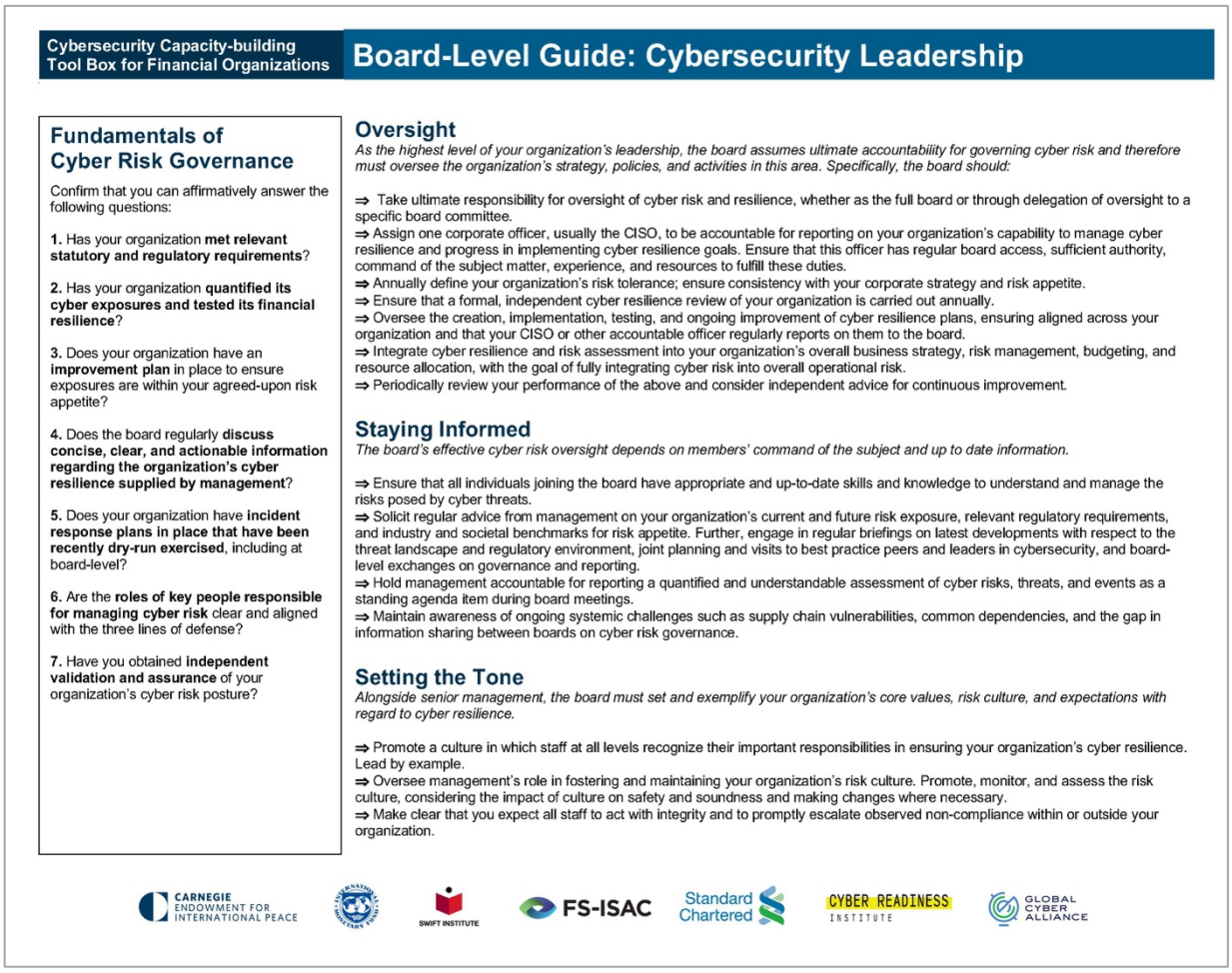
REVIEWING

- ☐ 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.

Supplementary Report

1. IN DETAIL: "Board-Level Guide: Cybersecurity Leadership"

Figure 2: Board-Level Guide: Cybersecurity Leadership



Boards of directors take ultimate responsibility for setting their organizations' broad policies, goals, and strategies. With cybersecurity being increasingly recognized as a pressing mainstream concern, it is critical that boards pay attention and ensure their organizations are resilient against cyber incidents. The recommendations in this section will help boards integrate cyber awareness into their organizations' overall business decisions and risk culture. Specifically, they advise boards on how to organize their personnel and policies, to stay informed of the threat landscape, and to assess their own progress and leadership.

Fundamentals of Cyber Risk Governance[11]

As the board, confirm that you can **affirmatively answer several fundamental questions** about the status of your organization's cybersecurity.

WHY: Reflecting on questions such as regulatory compliance, organization of personnel and policies, and incident response plans is important for the board to stay abreast of its organization's cyber risk and preparedness. Such awareness will allow the board to make proactive, informed decisions.

HOW: As the board, periodically (at least once annually) ask and document your answers to 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 organization's cyber resilience supplied by management?
- Does your organization have breach 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 and document your progress.

Oversight

As the highest level of your organization's leadership, the board assumes ultimate accountability for governing cyber risk and therefore must oversee the organization's strategy, policies, and activities in this area. Specifically, the board should:

Take ultimate responsibility for oversight of cyber risk and resilience, whether as the full board or through delegation of oversight to a specific board committee.[12]

WHY: The board must actively own its position as leader of its organization's cybersecurity activities in order to maintain continuity and accountability across the organization.

HOW: Acknowledge cybersecurity as a key business issue at board meetings and engage regularly with your CEO, CISO, and other relevant personnel about cyber activities, trends, and threats.

Use the questions found on page 9 of WEF's Cyber Resilience Principles and Tools to determine whether the board should retain primary responsibility for reviewing the management of cybersecurity, or whether it should designate a committee to do so:

- Is the board able to devote the time to consistently discuss cyber resilience matters, or do time constraints only permit for periodic updates?
- Does the board prefer to have discussions with management with respect to cyber resilience more frequently than regular scheduled board meetings?
- Does the company's industry warrant special attention to cyber resilience matters, and do industry practices or peer companies suggest use of specific governance structures? Does a regulatory or other oversight body or obligation currently exist?
- Would having a designated committee of specialized or interested members be beneficial to the review of the company's cybersecurity/ resilience strategy and the review of its management?

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.[13]

WHY: Having a CISO or another single officer who is responsible and accountable for managing your organization's cybersecurity goals, status, and activities gives the board a clear point of information and communication, simplifying its oversight and allowing management actions to be carried out uniformly.

HOW: Clearly define the officer's roles and responsibilities, including by answering the following questions from page 10 of WEF's Cyber Resilience Principles and Tools:

- Does the accountable officer have sufficient independence from IT to provide oversight reporting on overall matters of technology and cyber risk?
- Is there a need for multiple lines of review and audit?

Ensure that this officer has regular board access, sufficient authority, command of the subject matter, experience, and resources to fulfill their duties, including by answering the following questions from WEF's Cyber Resilience Principles and Tools (p. 10+11):

- To whom does the accountable officer in charge of cyber risk management report? What is the seniority of this officer?
- Are there clear communication and escalation pathways, processes, and thresholds for conflict resolution?
- Does the accountable officer have sufficient authority to drive a business and IT culture that builds suitable controls into the business and IT processes?
- Who makes decisions on sourcing of cybersecurity activities and resources?
- What percentage of your organization's annual operating expenditure is dedicated to cyber resilience and how does this compare with industry norms?
- Is there a dedicated cybersecurity budget, and, if so, who owns it?
- Are there other budgets contributing to your organization's cyber resilience, such as for IT or risk?
- Does your organization regularly benchmark its metrics against peers within and beyond the financial sector? Such metrics might include:
    - The percentage of your organization's annual revenue that is spent on cyber resilience,
    - The size of your cyber resilience team,
    - The percentage growth in your cyber resilience budget and resources over the past three years
    - The planned percentage growth in your cyber resilience budget and resource for the next three years, and
    - The maturity of your control operations.

Annually **define your organization's risk tolerance**, ensuring it is consistent with your corporate strategy and risk appetite.[14]

WHY: All cybersecurity actions taken by your organization and its individual personnel are informed by the amount of risk involved in those activities as weighed against the understood risk tolerance of your organization. It is the board's responsibility to define the

amount of risk that your organization is willing to take on in the course of pursuing its business objectives.

HOW: Ensure the board is advised by management on your organization's current and future risk exposure, regulatory requirements, and industry standards.

As the board, answer the following questions from pages 11-12 of WEF's Cyber Resilience Principles and Tools:

- Have you had the opportunity to understand the context of cybersecurity risk appetite? Consider that appetite may change with different company objectives in terms of balancing risk and the operational cost and impact of cybersecurity measures.
- Do you have visibility on how your stated risk appetite is being applied in your organization's decision-making?
- When decisions are made that exceed the bounds of your organization's risk appetite, are they presented back to you on an annual basis?
- Is risk examined on a case-by-case or business line basis as well as in the aggregate to ensure understanding of enterprise-wide risk?
- Do you have the necessary shareholder, regulatory, customer, and other external perspectives to allow you to set your organization's cyber risk appetite?
- Do you understand the real impact of cyber risk in business terms such as business disruption or impact on product and service quality or reputation?
- Where your organization supports critical national infrastructure or other national interests, do you have a strategy to deal with broader governmental and societal stakeholder expectations?
- Do you hold the accountable officer responsible for understanding the cyber risk in advance of undertaking new business ventures (e.g. mergers, acquisitions, joint ventures, and divestments) or new products or technologies?
- Does the accountable officer brief you on changes in customer, staff, or regulatory expectations or other external factors such as incidents or the views of society as a whole, which may change the risk appetite?

See the Board Cyber Risk Framework and Appendix 3 of WEF's Cyber Resilience Principles and Tools for more details on how the board can determine cyber risk appetite.[15]

Ensure that a **formal, independent cyber resilience review of your organization** is carried out annually.[16]

WHY: Independent assessments will help you understand your organization's cyber risks and vulnerabilities and subsequently prioritize actions to continuously improve resilience in line with your business objectives.

HOW: Task your CISO or other accountable officer with conducting or hiring an outside service to conduct a review of your organization's cybersecurity posture. Require that the results are promptly analyzed and presented to the board to inform any necessary changes to policies and/or activities

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.[17]

WHY: A key piece of your organization's cybersecurity posture is having appropriate, proactive, well-documented policies and plans in place to inform staff behavior and dictate response procedures. The board should ensure the formulation of such plans and stay updated on progress.

HOW: Instruct senior management to collaborate on cyber resilience plans for your organization and to keep you regularly updated on key progress and decision points. Such plans include having an organization-wide cybersecurity policy that is used to train all staff, as well as having incident response plans in place.

Ensure that your CISO takes on the role of implementing, testing, and assessing the effectiveness of such plans.

Integrate cyber resilience and risk assessment into your organization's overall business strategy, risk management, budgeting, and resource allocation.[18]

WHY: Cyber resilience being as important as it is to an organization's prosperity, your goal should be to fully integrate cyber risk into your organization's overall operational risk functions.

HOW: Familiarizing yourself with cyber risk is the first step to integrating it naturally into broader discussions and activities. Alongside such knowledge-enhancing activities, which are outlined

in detail the next section, make conscious efforts to include cybersecurity as a topic in as many board discussions as it is relevant.

Periodically **review your performance of the above** and consider seeking independent advice for continuous improvement.[19]

WHY: Just as you perform oversight of the rest of your organization's personnel and activities, you must maintain awareness of whether your board's own behavior aligns with your stated policies and goals.

HOW: As a board, set concrete goals for your cybersecurity engagement, such as defining the regularity of updates from management, engaging outside experts, and creating certain policies. Set a meeting, at least once annually, for the board to discuss its progress on these goals.

Staying Informed

The board's cyber risk oversight will only be effective if its individual members have command of the subject and the group as a whole is continuously consuming relevant information.

Ensure that **all individuals joining the board have appropriate and up-to-date skills and knowledge** to understand and manage the risks posed by cyber threats.[20]

WHY: The ability of the board to stay informed and perform its cybersecurity leadership duties depends on the knowledge and capabilities of its individual members.

HOW: The existing board should establish specific training for existing board members and criteria for the expected cybersecurity qualifications of new board members. These criteria do not need to be absolute – rather, if a desirable board member is identified who does not meet them, the board should work with either internal or external educators and toolkits to bring them up to speed. Your CISO and your organization-wide cybersecurity policy are good starting points to help determine criteria.

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.[21]

WHY: Receiving updates from your management team will be the primary lens through which you understand the status of your organization's cybersecurity.

HOW: Set a recurring requirement for management to brief the board on your organization's cybersecurity. Hold management accountable for reporting a quantified and understandable assessment of cyber risks, threats, and events as a standing agenda item during board meetings. Make sure the reporting is concise, clear, and actionable.[22]

Validate management's assessments with your own strategic risk assessment using WEF's Board Cyber Risk Framework.[23]

Engage in:

- Regular briefings on duties created by new regulations and legislation,[24]
- Board and executive committee joint planning, breach response programs, and visits to best practice peers and leaders in cybersecurity,[25]
- Security briefings on the threat environment, and[26]
- Board-level exchanges of information on governance and reporting.[27]

Maintain awareness of ongoing systemic challenges such as supply chain vulnerabilities, common dependencies, and the gap in information sharing between boards on cyber risk governance.[28]

WHY: No matter how much time, energy, and resources your organization dedicates to cybersecurity, some tough, systemic challenges will always remain unresolved and will continue to evolve and create risk. As such, the best strategy is to stay informed.

HOW: Task your management team with producing regular (at least annual) trend analyses, presenting actionable information on strategic and systemic challenges.

Setting the Tone

Alongside senior management, the board must set and exemplify your organization's core values, risk culture, and expectations with regard to cyber resilience.

Promote a culture in which staff at all levels recognize their important responsibilities in ensuring your organization's cyber resilience. Lead by example.[29]

WHY: Your organization's culture drives employee behavior, determining the safety and soundness of many aspects of your business. As such, you should take an active role in shaping it.

HOW: Discuss cybersecurity as part of your communication with staff to make clear that it is a priority. Ensure that your CISO or other accountable officer has thoroughly educated all staff on your organization's cybersecurity policies and procedures.

Oversee management's role in fostering and maintaining your organization's risk culture.[30] **Promote, monitor, and assess the risk culture**.[31]

WHY: An effective risk culture for your organization means that any risks taken are well informed and proportional to your agreed-upon risk appetite. As the determiner of your organization's risk appetite, you are crucial to fostering this culture.

HOW: Communicate your agreed-upon risk appetite to senior management for them to disseminate to staff. Require active reporting from management on the risks being taken in relation to cybersecurity, and reward informed and risk-appropriate decision making.

Make clear that you **expect all staff to act with integrity and to promptly escalate observed non-compliance** within or outside your organization.[32]

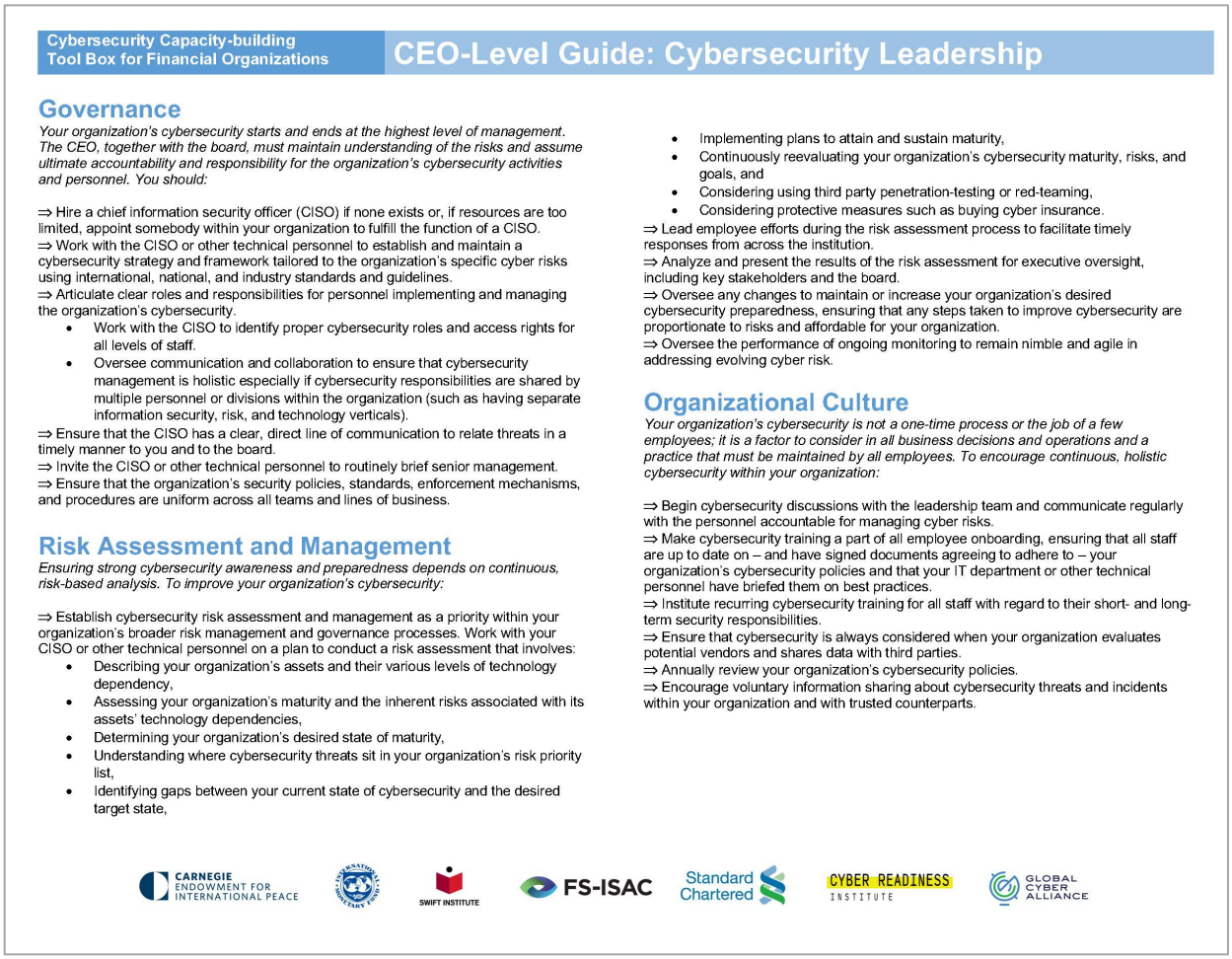
WHY: It must be instinctive for your staff to detect and quickly report all potential cybersecurity issues and incidents to the proper channels, which may include the ability for anonymous reporting. This allows your organization to properly follow incident response protocols.

HOW: When communicating with staff, use language of integrity and responsibility with regard to cybersecurity.

Ensure that your CISO has trained all new and current employees on your organization's cybersecurity policy, including incident response and reporting procedures.

2. IN DETAIL: "CEO-Level Guide: Cybersecurity Leadership"

Figure 3: CEO-Level Guide: Cybersecurity Leadership



Cybersecurity Capacity-building Tool Box for Financial Organizations

CEO-Level Guide: Cybersecurity Leadership

Governance

Your organization's cybersecurity starts and ends at the highest level of management. The CEO, together with the board, must maintain understanding of the risks and assume ultimate accountability and responsibility for the organization's cybersecurity activities and personnel. You should:

⇒ Hire a chief information security officer (CISO) if none exists or, if resources are too limited, appoint somebody within your organization to fulfill the function of a CISO.
⇒ Work with the CISO or other technical personnel to establish and maintain a cybersecurity strategy and framework tailored to the organization's specific cyber risks using international, national, and industry standards and guidelines.
⇒ Articulate clear roles and responsibilities for personnel implementing and managing the organization's cybersecurity.

- Work with the CISO to identify proper cybersecurity roles and access rights for all levels of staff.
- Oversee communication and collaboration to ensure that cybersecurity management is holistic especially if cybersecurity responsibilities are shared by multiple personnel or divisions within the organization (such as having separate information security, risk, and technology verticals).

⇒ Ensure that the CISO has a clear, direct line of communication to relate threats in a timely manner to you and to the board.
⇒ Invite the CISO or other technical personnel to routinely brief senior management.
⇒ Ensure that the organization's security policies, standards, enforcement mechanisms, and procedures are uniform across all teams and lines of business.

Risk Assessment and Management

Ensuring strong cybersecurity awareness and preparedness depends on continuous, risk-based analysis. To improve your organization's cybersecurity:

⇒ Establish cybersecurity risk assessment and management as a priority within your organization's broader risk management and governance processes. Work with your CISO or other technical personnel on a plan to conduct a risk assessment that involves:

- 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 using third party penetration-testing or red-teaming,
- Considering protective measures such as buying cyber insurance.

⇒ Lead employee efforts during the risk assessment process to facilitate timely responses from across the institution.
⇒ Analyze and present the results of the risk assessment for executive oversight, including key stakeholders and the board.
⇒ Oversee any changes to maintain or increase your organization's desired cybersecurity preparedness, ensuring that any steps taken to improve cybersecurity are proportionate to risks and affordable for your organization.
⇒ Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving cyber risk.

Organizational Culture

Your organization's cybersecurity is not a one-time process or the job of a few employees; it is a factor to consider in all business decisions and operations and a practice that must be maintained by all employees. To encourage continuous, holistic cybersecurity within your organization:

⇒ Begin cybersecurity discussions with the leadership team and communicate regularly with the personnel accountable for managing cyber risks.
⇒ Make cybersecurity training a part of all employee onboarding, ensuring that all staff are up to date on – and have signed documents agreeing to adhere to – your organization's cybersecurity policies and that your IT department or other technical personnel have briefed them on best practices.
⇒ Institute recurring cybersecurity training for all staff with regard to their short- and long-term security responsibilities.
⇒ Ensure that cybersecurity is always considered when your organization evaluates potential vendors and shares data with third parties.
⇒ Annually review your organization's cybersecurity policies.
⇒ Encourage voluntary information sharing about cybersecurity threats and incidents within your organization and with trusted counterparts.

There has been a growing consensus in recent years resulting from high profile incidents and the continuously deteriorating cybersecurity landscape that cybersecurity must start at the top. An organization's CEO must take the lead in cybersecurity, developing awareness of their organizations' cyber risk, setting organizational priorities and policies to deal with that risk, and acting as the head of their organization's body of cybersecurity personnel. The recommendations in this section therefore discuss these cybersecurity leadership responsibilities in greater detail and outline a set of activities for executives to help them think about cybersecurity more holistically and as part of broader organizational strategy.[33]

Governance

CEOs assume ultimate responsibility for structuring and overseeing their organization's cybersecurity policies and personnel. The main cybersecurity governance functions for CEOs are overseeing the development of and adherence to a cybersecurity risk management and policy program and establishing clear communication with technical personnel. Specifically:

Hire a chief information security officer (CISO) if none exists or, if resources are too limited, appoint somebody within your organization to fulfill the function of a CISO.

WHY: The role of the CISO is central to an organization's cybersecurity operations and management. For example, in 2017, India's Ministry of Electronics and IT required all ministries/departments/organizations to nominate a CISO to establish their cyber security programs, coordinate compliance, and manage information-sharing.[34] The CISO occupies a leadership role, taking responsibility for driving and managing their organization's information security efforts. Having a CISO allows the organization to make and enforce policies, govern practices and personnel, and manage risks in a structured way.

HOW: Your CISO should be a member of senior management and should report directly to the CEO or other senior most person. See resources such as the list from India's Electronics and IT Ministry for descriptions of the proper roles and responsibilities of CISOs.[35]

Work with the CISO or other technical personnel to **establish and maintain a cybersecurity strategy and framework** tailored to the organization's specific cyber risks using international, national, and industry standards and guidelines.[36]

WHY: Having a comprehensive cybersecurity strategy in place is the first step in responsible cybersecurity management for an organization. It helps to define priorities, roles, responsibilities, and expectations at both the technical and behavioral level. The strategy will act as a touchstone for all future activity, from employee training to capacity building to incident response.

HOW: To understand what must be included in their cybersecurity strategy, organizations must review any regulations to which they are subject. The Financial Stability Board and the World Bank have produced comprehensive digests of cybersecurity regulations affecting the financial sector.[37]

Financial sector-specific entities like the Federal Financial Institutions Examination Council and the Financial Services Sector Coordinating Council have published "profiles to help

financial institutions understand their particular risks and responsibilities in cybersecurity.[38] Additionally, organizations like the U.S. National Institute of Standards and Technology and the International Organization for Standardization have released comprehensive guidance on assessing cybersecurity risk and subsequently developing policies.[39] We recommend using these documents to develop a cybersecurity strategy.

Articulate **clear roles and responsibilities for personnel** implementing and managing the organization's cybersecurity.[40]

WHY: Staff must understand their required responsibilities under your organization's cybersecurity policies so they can fully perform their duties and so management can hold the proper personnel responsible for various tasks.

HOW: Work with the CISO to identify proper cybersecurity roles and access rights for all levels of staff. Include provisions in the organization's cybersecurity strategy defining the expectations for technical personnel, leadership, and general employees and have all staff sign written documents confirming they understand their roles. Oversee communication and collaboration to ensure that cybersecurity management is holistic especially if cybersecurity responsibilities are shared by multiple personnel or divisions within the organization (such as having separate information security, risk, and technology verticals).

Ensure that the CISO has a clear, direct line of communication to the CEO and board.

WHY: The CISO must be able to relate threats to other senior leadership in a timely manner.

HOW: Make clear to the CISO how the CEO and board prefer to be notified and encourage open communication. Plan for how the CEO will notify the board in case of incidents.

Invite the CISO or other technical personnel to routinely brief senior management.

WHY: Senior leadership must stay informed of developing needs, vulnerabilities, and incidents to properly allocate attention and resources to cybersecurity.

HOW: Plan regular briefings from your CISO in your calendar and make clear that it is a key responsibility of technical personnel to communicate developments with leadership.

Ensure that the organization's security policies, standards, enforcement mechanisms, and procedures are uniform across all teams and lines of business.[41]

WHY: The organization's cybersecurity must be approached holistically and therefore must be and internalized throughout the entire organization in an integrated manner.

HOW: Distribute the same cybersecurity strategy and policies to all teams and task the organization's technical personnel with ensuring uniform compliance. If an organization operates in multiple countries, aim to develop a coherent uniform cybersecurity strategy with jurisdiction-specific additions where needed.

Risk Assessment and Management

Establishing and maintaining strong cybersecurity awareness and preparedness for an organization depends on continuous, risk-based analysis. To improve the organization's cybersecurity:

Establish **cybersecurity risk assessment and management** as a priority within the organization's broader risk management and governance processes.[42]

WHY: Developing a risk-based cybersecurity program is the best way to approach this area.

HOW: Work with the CISO or other technical personnel to develop a plan to conduct an assessment of the organization's cybersecurity risk that involves:

- Describing the organization's assets and their various levels of technology dependency,
- Assessing the organization's maturity and the inherent risks associated with its assets' technology dependencies,
- Determining the organization's desired state of maturity,
- Understanding where cybersecurity threats sit in the organization's risk priority list,[43]
- Identifying gaps in alignment between the 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,[44]
- Considering using third party penetration-testing or red-teaming,
- Considering protective measures such as buying cyber insurance.

The CEO should lead employee efforts during the risk assessment process to facilitate timely responses from across the institution.[45]

The CEO should analyze and present the results of the risk assessment for executive oversight, including key stakeholders and the board.[46]

Oversee any changes to maintain or increase the organization's desired cybersecurity preparedness, ensuring that any steps taken to improve cybersecurity are proportionate to risks and affordable for the organization.[47]

Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving cyber risk.[48]

Organizational Culture

An organization's cybersecurity is not a one-time process or the job of a few employees but to be considered in all business decisions and operations and a practice that must be internalized by all employees. To encourage continuous, holistic cybersecurity within the organization:

Begin cybersecurity discussions with the leadership team and communicate regularly with the personnel accountable for managing cyber risks.[49]

WHY: When executives discuss and stay abreast of cybersecurity risk, planning, and resources, it helps integrate cybersecurity into regular business practices.

HOW: Put cybersecurity, including regular briefings from the CISO, on the CEO and board's agenda. Ask about cybersecurity considerations during broader management of organizational risk, planning, and budgeting.

Make cybersecurity training a part of all employee onboarding, ensuring that all staff are up to date on – and have signed documents agreeing to adhere to – your organization's cybersecurity policies and that your IT department or other technical personnel have briefed them on best practices. Institute **recurring cybersecurity training for all staff** with regard to their short- and long-term security responsibilities.[50]

WHY: Holistic cybersecurity management requires all employees to be constantly aware and well-versed in the organization's policies and procedures. Ensuring that they have signed

commitments to adhere is a necessary starting point to make all employees feel responsible for their part in cybersecurity.

HOW: Direct the organization's human resources and technology teams to work together to make cybersecurity a part of all employee onboarding to get all staff up to date on – and signed documents agreeing to adhere to – the organization's cybersecurity policies and brief them on best practices. Direct human resources and technology teams to develop an annual or more regular cybersecurity update for all personnel that is informed by your organization's policies.

Ensure that **cybersecurity is always considered when your organization evaluates potential vendors and shares data with third parties**.

WHY: Every new technology dependency or data sharing arrangement your organization engages in presents a new vector for potential cyber risk. Ensure that the organization's cybersecurity policies extend to and inform relationships with vendors and peer institutions with which data is shared.

HOW: Require in vendor onboarding procedures that cybersecurity be considered. Direct an personnel responsible for evaluating and hiring vendors to consider the recommendations in the Third Party section of this paper.

Annually review the organization's cybersecurity policies.

WHY: An organization's policies must be holistic and dynamic to keep up with changing needs, practices, and threats.

HOW: Direct the CISO to develop an annual report of incidents, trends, and vulnerabilities and to have an annual discussion with technical personnel. The CISO should then present insights to be reviewed by management and the board.

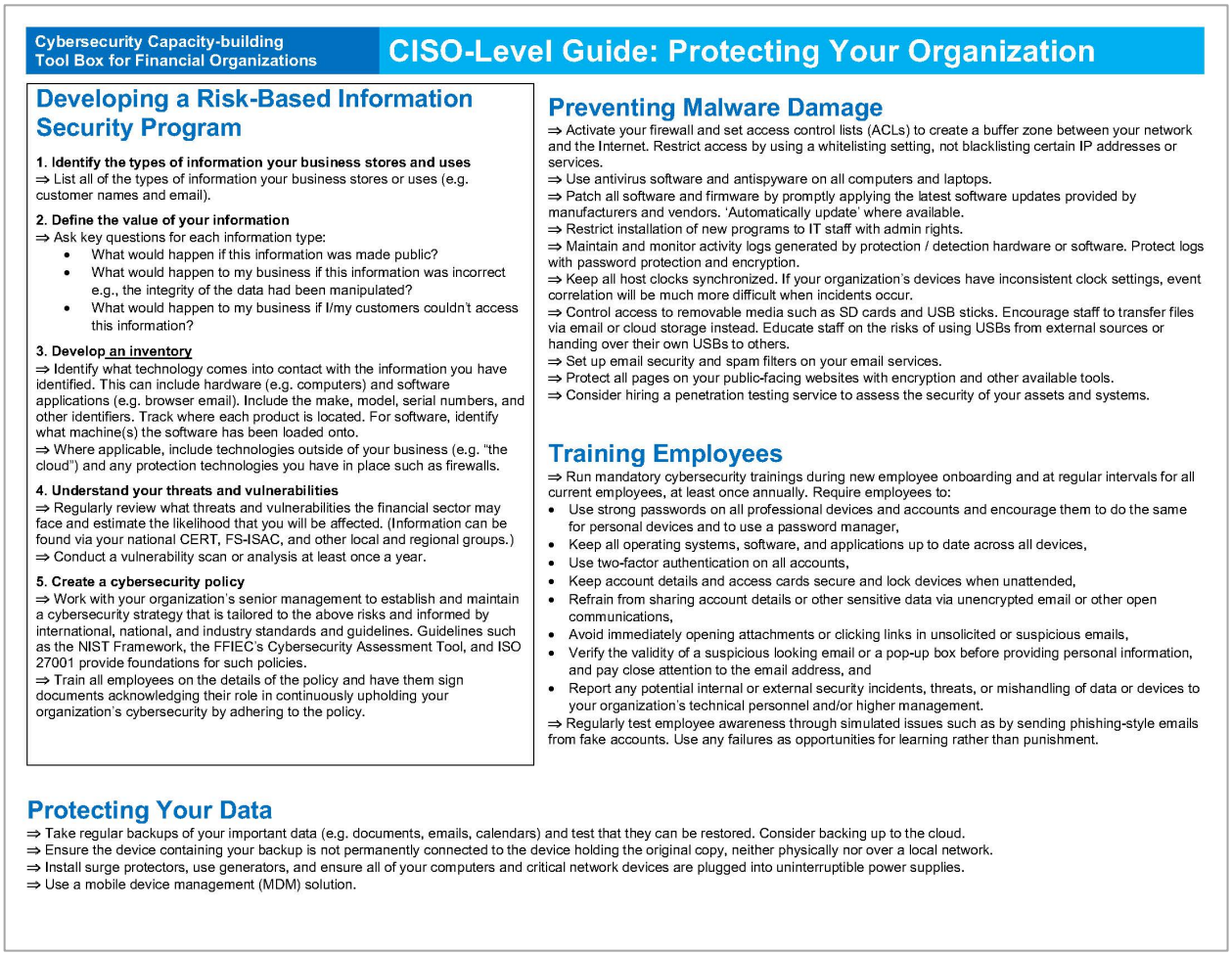
Encourage voluntary information sharing about cybersecurity threats and incidents within your organization and with trusted counterparts.

WHY: Voluntary information sharing builds a community of trust between organizations and within industries that enables collective monitoring and responsiveness to cyber threats. Establishing the criticality of this practice will empower the organization's technical personnel to engage with other organizations.

HOW: Ensure that information sharing is included as an element of the organization's cybersecurity policy, and encourage the CISO to engage in industry-based information sharing and collaboration programs such as the FS-ISAC as well as other national or regional programs.[51] FS-ISAC is a global non-profit resource for the financial industry that provides threat and vulnerability information, conducts exercises and offers trainings, manages industry-wide rapid-response communications, and fosters collaboration with other sectors and government agencies.[52] The U.S. NIST also offers a comprehensive guide on how to engage in cyber threat information sharing.[53]

3. IN DETAIL: "CISO-Level Guide: Protecting the Organization"

Figure 4: CISO-Level Guide: Protecting Your Organization



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.

Baseline cybersecurity best practices are well understood and available. They key challenge remains to ensure their adoption at scale. Building on existing work, this section presents a package of core categories and recommendations for essential cybersecurity protections to which organizations should adhere.

Developing a Risk-Based Information Security Program[54]

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

WHY: Understanding and managing your organization's cyber risk starts with knowing your information landscape.

HOW: Create a master document listing all types of information, both internally produced (emails, documents) and externally collected (customer data such as names and email addresses).

2. Define the value of your information.

WHY: Assessing the importance of each area of information your organization handles will allow you to prioritize cybersecurity measures to target the greatest risk areas.

HOW: Ask and record in your master document the answers to the following 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?
- What would happen to my business if I/my customers couldn't access this information?

3. Develop an inventory.[55]

WHY: Each information type's associated risk depends on how it is exposed to various internal and external technologies and systems. Identifying these intersections helps you further develop awareness of your information and risk landscape.

HOW: Identify and record in your master document what technology comes into contact with each group of 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 for each technology.
- Track where each product is located. For software, identify what machine(s) the software has been loaded onto.

4. Understand your threats and vulnerabilities.

WHY: Your organization's cybersecurity planning and policies should be based on knowledge of the actual most pressing risks (threats and vulnerabilities) your organization (and others like it) faces.

HOW: Regularly review what threats and vulnerabilities the financial sector may face by following updates from your national CERT, FS-ISAC, and other international and national information sharing and threat intelligence hubs.[56] Estimate the likelihood you will be affected based on whether technologies or practices that your organization uses have been identified as vulnerable.

Consider hiring a cybersecurity company to conduct a vulnerability scan or analysis at least once a year.

5. Create a cybersecurity policy.

WHY: To approach cybersecurity in a holistic and organized way, your organization must clearly document its basic priorities and policies.

HOW: Work with your organization's senior management to establish and maintain a cybersecurity strategy and framework that is tailored to the above risks and is appropriately informed by international, national, and industry standards and guidelines.[57] Guidelines such as the NIST Framework, the FFIEC's Cybersecurity Assessment Tool, and ISO 27001 provide templates, categories, and details for building out and improving such policies. Various regulatory regimes offer guidelines detailing what compliance is expected of organizations under their supervision.[58]

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[59]

Activate your **firewall and set access control lists (ACLs)**. Restrict access by **using a whitelisting setting**, not blacklisting certain IP addresses or services.

WHY: Using these security measures will create a buffer zone between your network and the internet by filtering traffic.

HOW: Enable firewall in the settings on your organization's computer networks and within any antivirus software you use. Consider using ACLs on each router or switch in your network to control access to network resources.[60]

Use **antivirus software and antispyware** on all computers and laptops.[61]

WHY: Having antivirus and antimalware detection programs in your systems offers an important first line of notification and defense against cyber incidents.

HOW: Search for available services and then ask the questions listed in the Third Parties section later in this paper on How to Choose Vendors.

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.[62]

WHY: Software and firmware updates are regularly released to mitigate identified vulnerabilities. Promptly installing updates will prevent your organization from falling behind and becoming a target of attackers exploiting known vulnerabilities.

HOW: Check the settings options offered by all existing and new manufacturers and vendors for 'auto update' and use that feature where possible. If automatic updates are not available, identify or establish a communication channel or notification outlet to ensure you are notified of new updates.

Maintain and monitor activity logs generated by protection / detection hardware or software.[63] Protect logs with password protection and encryption.

WHY: Logs are records of the running state of hardware and software on your organization's networks. Log management ensures that your organization possesses proper, detailed security records to help identify security incidents and other problems.[64]

HOW: Log management can be complicated and difficult due to the high volume of log data being constantly produced and the limited resources with which to constantly analyze them. Consult detailed guides for strategies to approach this challenge and get the most out of log management.[65]

Keep all host **clocks synchronized**.

WHY: If your organization's devices have inconsistent clock settings, event correlation will be much more difficult when incidents occur.[66] During incident response, you will need an accurate timeline of events and steps taken.

HOW: Protocols such as the Network Time Protocol (NTP) can be used to synchronize clocks among hosts.[67]

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.[68]

WHY: Removable media can be loaded with malware if not obtained from secure sources. It would be difficult to assess the provenance of all outside media, so it is safer to reduce usage.

HOW: Do not hand out removable media and inform staff during trainings to restrict use of these devices.

Set up **email security and spam filters** on your email services.[69]

WHY: Filters will block many obvious and dangerous forms of phishing and other email attacks.

HOW: Work with your email provider to set desired filters. Consider implementing DMARC.

Protect all pages on your public-facing websites with encryption and other available tools.[70]

WHY: Public web apps are where customers input login credentials and other sensitive information. They are the most visible of your organization's systems and as such require extra security attention.

HOW: See the section on Customer Security for details on protecting public web applications, including using HTTPS, managing cookies settings, using public key pinning, and having content policies.

Consider hiring a **penetration testing service to assess the security of your organization's assets and systems**.

WHY: Penetration testing helps you identify and plan to mitigate vulnerabilities. Though this can be costly and should be weighed against other budgetary considerations, penetration testing can offer invaluable insights for protecting against incidents.

HOW: Many cybersecurity companies offer penetration testing services. Use the questions in the Third Party section of this paper to evaluate potential vendors, and work with leadership to assess the viability of hiring such services.

Training Employees

Run **mandatory cybersecurity trainings** during new employee onboarding and at regular intervals for all current employees, at least once annually.

WHY: Human error accounts for a significant proportion of an organization's cybersecurity risk. All employees must consider themselves to be crucial to the organization's security, and must be equipped with best practices for their individual behavior.

HOW: Advise[71] 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,
- 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.
- Exercise particular caution when traveling e.g., with respect to airport or hotel networks, typing your passwords in public spaces, etc.

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[72]

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.[73]

WHY: Having up-to-date, secured backups will allow you to maintain business continuity and restore your assets in the event of an incident affecting the availability or integrity of your data.

HOW: There is a variety of options for backup data storage, including direct attached storage (DAS), network attached storage (NAS), disaster protected storage, Cloud online storage, and offline media.[74] Consult publicly available information about evaluating such options, and then request documentation of cybersecurity compliance and protocols from your selected provider(s).[75] Consider using multiple methods.

Ensure the device containing your **backup is not permanently connected to the device holding the original copy**, neither physically nor over a local network.

WHY: Maintaining segmentation of backup storage helps prevent one incident from disrupting or eliminating all data at once.

HOW: Keep at least one backup on offline drives or in Cloud storage.

Install surge protectors, use generators, and ensure all of your computers and critical network devices are plugged into uninterruptible power supplies.[76]

WHY: This will prevent disruptions such as power outages from interrupting your operations or erasing data.

HOW: Purchase sufficient energy protection tools to prevent damage caused by outages.

Use a **mobile device management (MDM)** solution.

WHY: MDM is the deployment of on-device applications and organizational policies to allow your IT teams to ensure compliance across organization-owned and employee-owned devices being used on your networks.

HOW: Hire a MDM solution provider and install its software on all of your organization's mobile devices. Require all employees to install the necessary applications and configurations on any personal devices they plan to connect to your networks.

Keeping Your Devices Safe[77]

Switch on **PIN and password protection** for mobile devices.

WHY: This simple authentication step will help prevent would-be attackers from accessing the contents of stolen devices.

HOW: Look in device settings to enable these protections.

Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.

WHY: This will reduce the risk of unauthorized systems or data access by criminals who have stolen one of your organization's or employee's devices.

HOW: Most device makers provide some sort of device tracking service. Using them requires device owners to enable the "find my device" feature in advance on the device. For example both Apple's Find My iPhone and Google's Find My Device tools offer tracking and remote locking services.[78]

Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.[79]

WHY: Software updates for devices and apps are published regularly to mitigate identified bugs and vulnerabilities. Promptly installing these updates will prevent devices from being targeted by hackers exploiting known vulnerabilities.

HOW: Most mobile devices offer an "auto update" feature for all installed applications. Update the software of the device itself when new updates are announced by the device maker.

When sending sensitive data, don't connect to public Wi-Fi hotspots – use cellular connections (including tethering and wireless dongles) or use VPNs.

WHY: Many public Wi-Fi hotspots, especially ones that are not password-protected, may have low security standards and thus are hotbeds for snooping and other malicious activity that could target your organization's transactions.

HOW: Be aware of your mobile device settings that may automatically connect you to public Wi-Fi. Pause before sending sensitive data to ensure you are not using public Wi-Fi and instead are relying on cell service.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

WHY: Out of date devices will no longer receive software and firmware updates from manufacturers to protect against newly identified bugs and vulnerabilities. This could leave your organization at risk.

HOW: Regularly follow news updates and information from your device manufacturers to check whether your devices are supported.

Set reporting procedures for lost or stolen equipment.

WHY: Lost or stolen equipment in the hands of bad actors poses an acute threat to the confidentiality of your systems, especially if the equipment can be unlocked easily (it should not, though, if the other steps here have been followed). As such, your organization needs to be able to find out as soon as possible about missing devices to activate remote tracking and locking features and to take any other necessary protection measures.

HOW: Inform employees during cybersecurity trainings of their duty to report lost or stolen equipment as soon as possible to you or other technical personnel. Include provisions about lost or stolen equipment protocols in your organization's cybersecurity policy.

Using Passwords[80]

Make sure all computers **use encryption products that require a password to boot**. Switch on **password or PIN protection for mobile devices**.

WHY: Passwords are a simple and helpful (if imperfect) layer of initial security and authentication, and should be used wherever possible with the highest level of strength. They are especially helpful in the case of physical theft of devices.

HOW: Use device settings to enable password protection wherever possible.

Use strong passwords, avoiding predictable passwords (like passw0rd) and personal identifiers (such as family and pet names). Instruct all employees to do the same.[81]

WHY: Common, insecure passwords are well-documented and well-exploited by hackers. In 2018, SplashData estimated that 10 percent of people use at least one of its published list of the 25 most common (worst) passwords such as "123456," "password," and "qwerty."[82]

HOW: Follow current best thinking on password generation. Current recommendations focus on longer sequences of words that are not easily guessable but are easier to remember than a random string of letters, numbers, and symbols.[83]

Use **two factor authentication (2FA)** wherever possible.[84]

WHY: This kind of multi-layer authentication prevents man-in-the-middle attacks and generally promotes a higher level of account security.

HOW: Many services to which users are required to log in, such as email accounts, social media, and other tools, have options in their settings to enable 2FA. You can also hire a multifactor authentication solution service to set up 2FA for your system and compute accounts for all employees.

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

WHY: Hackers can take advantage of patterns and existing knowledge of default passwords for various technologies to gain access. Use new, unique passwords for better security.

HOW: Devices should have clear features to change passwords. If not, contact the manufacturer.

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).

WHY: In case of a suspected breach or attack, users will need to be able to change their passwords to prevent new or continued account access.

HOW: Provide employees with step-by-step instructions to change their passwords during trainings and in written form.

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.[85]

WHY: Using a password manager eliminates the need to remember many different passwords by securely storing unique passwords for all accounts to be accessed via one "master password" (which, understandably, must be strong and highly secret). This eliminates the urge many people have to reuse the same password across many accounts or to create predictable variations.

HOW: Search and sign up for a password manager for businesses. Example services are 1Password and Lastpass.[86]

Controlling Permissions[87]

Ensure that all personnel have **uniquely identifiable accounts that are authenticated each time they access** your systems.[88]

WHY: This allows you visibility into individual users and sessions to more easily track incidents and fix security issues with particular accounts and personnel.

HOW: Set up individual log-ins for all employees and set computers to require log-in each time they are used.

Only give **administrative privileges to trusted IT staff and key personnel**.[89]

WHY: Most staff should not need to frequently alter computer or network settings or install new software. The security benefit usually outweighs the inconvenience of requiring employees to get permission from technically trained staff for these activities when necessary.

HOW: Train key personnel on how to manage admin privileges. Instruct all staff to go through IT to make computer system changes or additions.

Revoke administrator privileges on workstations for standard users.

WHY: This is the principle of least privilege, reducing risk by reducing the exposure of your data and systems to superfluous access and activity.

HOW: Use computer settings to limit access to admin privileges.

Only give employees access to the specific data systems that they need for their jobs and ensure they cannot install any software without permission.

WHY: This is the principle of least privilege, reducing risk by reducing the exposure of your data and systems to superfluous access and activity. This includes strict protocols with respect to former employees and swiftly blocking access for fired employees.

HOW: Obtain and use specific job descriptions for each employee when setting up accounts, only granting access to directly relevant data, systems, and operations. Set up systems so that only technical personnel or other admins can install software, requiring the rest of staff to request permission for specific additions.

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

WHY: This will ensure that you can control and monitor that only specific, authorized personnel are accessing your computers and sensitive areas.

HOW: Configure workplace computers so that employees must log in with their own unique credentials.

Use physical security measures such as ID badges and passcodes on doorways and elevators to protect the office premises, data centers, and sensitive areas such as technical rooms with network devices and cabling from unauthorized access.

Securing Your Wi-Fi Networks and Devices

Make sure your workplace **Wi-Fi is secure and encrypted** with WPA2.[90]

WHY: Many employees and customers will conduct important transactions and send sensitive information via your organization's wireless network. An unsecured Wi-Fi network puts this activity at risk of threats such as sniffing (stealing sensitive information that is not encrypted), evil twin attacks (setting up a fake network access point impersonating yours to read transactions), and piggybacking/wardriving (outsiders connecting to your network and conducting illegal activity).[91] Hackers are also adept at exploiting many default router settings such as remote management and passwords. As such, you should take advantage of all available settings to encrypt, hide, password protect, and update your organization's wireless network.

HOW: Routers often come with encryption turned off, so make sure to turn encryption on.[92] Consult information and options available from your wireless provider on how to do this. Usually, you can log into your router's configuration page (by typing the router's IP address into the search bar in your browser) and find the wireless encryption settings.[93]

Password protect access to the router, and make sure that the password is updated from the pre-set default.[94]

HOW: Log into your router's configuration page and update the password.

Turn off any "remote management" features.[95]

HOW: Some routers will have the option to allow remote access to your router's controls to allow the manufacturer to provide technical support. Log into your router's configuration page and make sure any of these settings are turned off.

Set up your wireless access point or router so it **does not broadcast the network name**, known as the Service Set Identifier (SSID).[96]

HOW: Log into your router's configuration page and adjust the settings to disable SSID broadcasting.

Limit access to your Wi-Fi network by only allowing devices with certain media access control addresses. If you want to provide customers with Wi-Fi, set up a separate public network.[97]

HOW: Use your router's settings to monitor and control which devices are accessing the 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.[98]

HOW: Log into your router's configuration page and find the DHCP section, make sure it I enabled.

Log out as administrator after you've set up the router.[99]

HOW: Log out of the router whenever you are done making changes to prevent piggybacking.

Keep your router's software up to date.

HOW: Go to your wireless provider's website and register using your router's model information. This will allow you to receive information about updates.[100] To update your router, log into your router's configuration page, find the update section, and download the update.

Avoiding Phishing Attacks[101]

Ensure staff **don't browse the web or check emails on servers or from an account with Administrator privileges.**

WHY: This control, in the case of an employee falling prey to a phishing attack, will prevent the attack from affecting universal accounts that could provide the attacker with more sensitive information and access more quickly.

HOW: Train and require any personnel with administrative privileges not to browse the web or check emails from admin accounts. Or, on the technical side, you can entirely disable email and browsing capabilities on admin accounts.

Set up **web and email filters.**[102]

WHY: This will block many suspicious and malicious emails and links before employees can access them and cause potential harm.

HOW: Work with your cybersecurity providers of antimalware and other services. Adjust settings via your email provider.

Consider blocking employees from visiting **websites commonly associated with cybersecurity threats.**[103]

WHY: This will prevent employees from even accidentally accessing known swaths of malicious content, an easy and high-yield step.

HOW: Work with your cybersecurity provider(s) on web filtering options.

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?

WHY: Phishing is a dangerous threat to your organization because it can take advantage of any of your employees' human error as a vector. As such, all staff must understand their responsibilities to be vigilant and report suspicious activity.

HOW: Provide all employees details and examples of common signs of phishing such as: unexpected and unsolicited messages; requests for personal information; altered email addresses; requests to install applications, enable macros, or adjust settings; spelling or other errors; mismatch

between sender address and signature; multiple recipients; and lack of personal address to recipient.[104]

Run a phishing test on your employees by setting up and sending a suspicious, phishing style message to all staff and tracking who opens it and clicks on the link.[105] Work with results to improve awareness among employees who fell for the trap.

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.

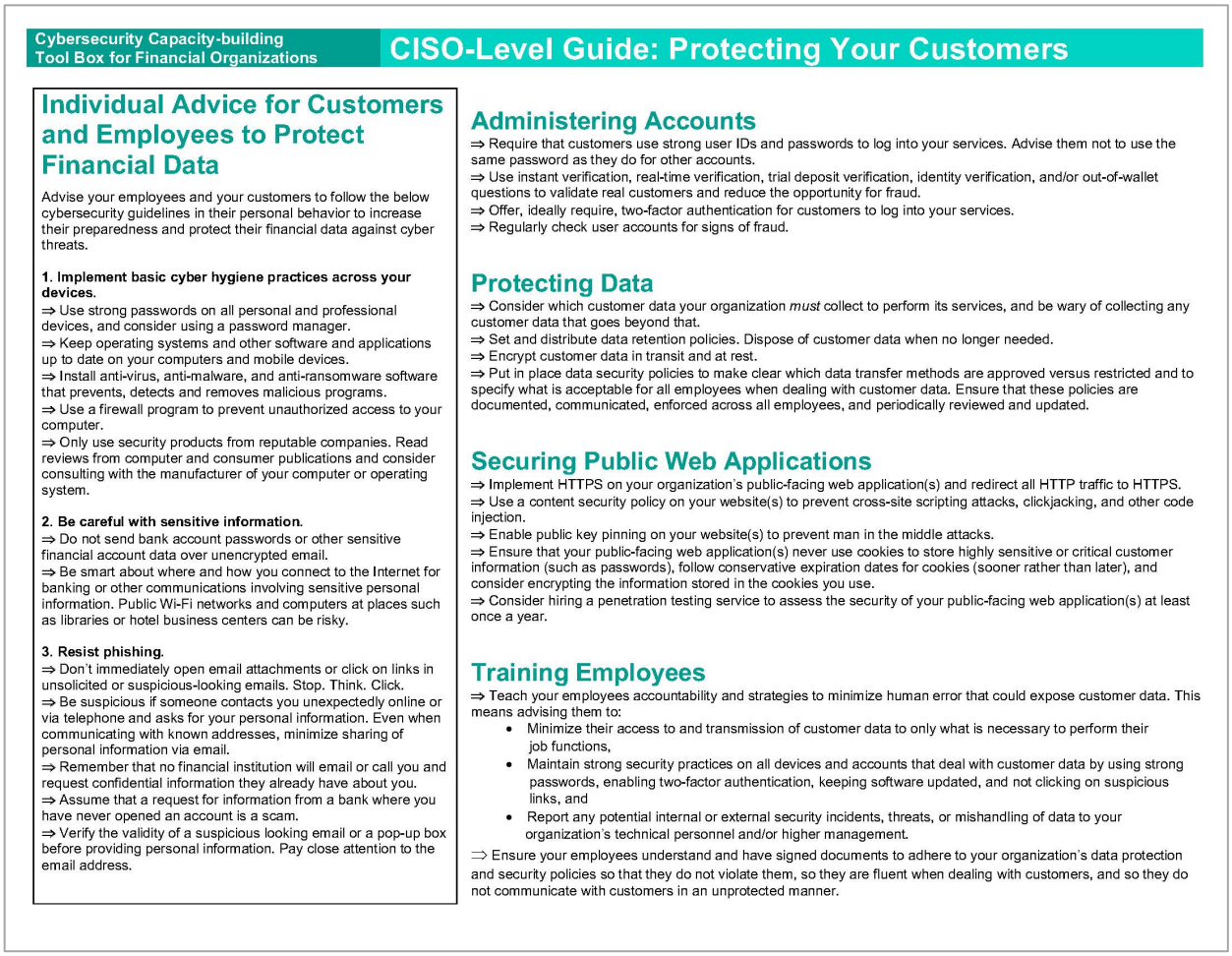
WHY: Phishing can lead to attackers stealing account information and/or installing malware, so take precautionary steps whenever such activity is suspected.

Punishing staff when incidents occur will likely discourage them from reporting in the future.

HOW: Instead of punishing staff, treat incidents as opportunities for learning – make sure they are aware of what specifically occurred and what to look out for in the future.

4. IN DETAIL: "CISO-Level Guide: Protecting Customers"

Figure 5: CISO-Level Guide: Protecting Your Customers



Cybersecurity Capacity-building Tool Box for Financial Organizations

CISO-Level Guide: Protecting Your Customers

Individual Advice for Customers and Employees to Protect Financial Data

Advise your employees and your customers to follow the below cybersecurity guidelines in their personal behavior to increase their preparedness and protect their financial data against cyber threats.

1. Implement basic cyber hygiene practices across your devices.
⇒ 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 your 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.

2. 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. Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky.

3. Resist phishing.
⇒ 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, 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 have 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, ideally require, two-factor authentication for customers to log 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 which 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 across all employees, 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) to prevent cross-site scripting attacks, clickjacking, and other code injection.
⇒ Enable public key pinning on your website(s) to prevent man in the middle attacks.
⇒ Ensure that your public-facing web application(s) never use cookies to store highly sensitive or critical customer information (such as passwords), follow conservative expiration dates for cookies (sooner rather than later), and consider encrypting the information 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 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 so that they do not violate them, so they are fluent when dealing with customers, and so they do not communicate with customers in an unprotected manner.

A particular responsibility in cybersecurity for financial organizations is to protect customer information and transactions. Much of the stability of the financial system as a whole depends on trust, so demonstrating robust data security to your customer base is crucial. The following recommendations focus on organizational best practices to for managing customer accounts and data, while also providing tips for communicating with and informing customers directly to enhance trust and encourage cyber hygiene.

Administering Accounts

Require that customers use **strong user IDs and passwords to log into your services.**

WHY: Customers' financial accounts are filled with valuable identifiers and financial data that are valuable to attackers. Strong passwords to protect those accounts are essential. Your organization should make clear to customers that it upholds a high level of security and expects customers to do the same.

HOW: Require customers to log into your public facing web applications each time they seek to access their accounts. Configure settings in those applications to require a minimum password length of 8 characters and include instructions on the page about how customers should set passwords. 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.[106]

WHY: These technical verification steps help to validate real customers and reduce the opportunity for fraud.

HOW: Third party technologies offer these verification layers that you can integrate into your web applications. FS-ISAC's guide offers descriptions of these different kinds of verification.

Offer, ideally require, two-factor authentication for customers to use when logging into your services.

WHY: Additional verification steps prevent fraud and other attacks.

HOW: Work with your organization's web developers, whether in-house or external, to enable 2FA for customers when logging in.

Regularly **check user accounts for signs of fraud**.[107]

WHY: Early and accurate fraud detection is a key service for customers, who may not always be aware that their credentials have been stolen and their account is being accessed.

HOW: Use automated and manual standard industry processes, such as reconciling accounts on a daily basis, to monitor customer accounts and transactions for suspicious activity.[108]

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.[109]

WHY: While the age of big data encourages high volumes of data collection, financial institutions should be wary of collecting and holding more customer information than they need. This is because the more information you hold, the more you have to lose and be responsible for in case of a cyber incident.

HOW: Apply the principle of least privilege to yourself as an organization, approaching customer services and accounts with the intention to only gather the information required to perform your duties.

Set and distribute data retention policies.

WHY: Your organization's protection of customer data not only involves the collection of that data, but also the protection of it while it is retained and the responsible and timely disposal of it when no longer needed.

HOW: Your policy should require that your organization dispose of customer data when no longer needed. Include this policy in your staff cybersecurity trainings.

Encrypt customer data in transit and at rest.

WHY: Encryption prevents unauthorized access to customer information by making it unreadable to any party not in possession of the access keys. Encryption is essential for customer data, especially for storing account log-in credentials.

HOW: A variety of encryption services are available for online applications and within storage solutions. Work with your organization's database managers and any vendors that deal with data storage and transfer to enable encryption.[110]

Put in place customer **data security policies**.

WHY: Employees must understand and feel responsible for protecting customer data in transit and at rest.

HOW: Make clear what data transfer methods are approved versus restricted. Specify what is acceptable for all employees when dealing with customer data. Ensure that these policies are documented, communicated, enforced, and periodically reviewed and updated.[111] Set and distribute data retention policies. Dispose of customer data when no longer needed.

Securing Public Web Applications

Implement HTTPS on your organization's public-facing web application(s) and redirect all HTTP traffic to HTTPS.[112]

WHY: HTTPS is a secure version of the protocol that allows data to be exchanged between users and web applications. This will protect your customers' interactions with your webservices.

HOW: Configuring HTTPS requires you to purchase an SSL certificate. This can be done through your domain service or through a third party. Once you have a certificate, you can enable and require HTTPS through your web developer.

Use a **content security policy** on your website(s).[113]

WHY: This is an added layer of security that prevents cross-site scripting attacks, clickjacking, and other code injection.

HOW: Work with web developers to configure your web server to enable a content security policy for handling traffic.

Enable public key pinning on your website(s).[114]

WHY: This security feature decreases the risk of man-in-the-middle attacks by blocking forged certificates.

HOW: Work with web developers to configure your web server to enable public key pinning.

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.[115]

WHY: Cookies are small files stored by websites to identify users and safe information. They can be manipulated by attackers, though, and as such your organization should have a secure strategy for using cookies.

HOW: Work with web developers to manage cookie settings.

Consider hiring a **penetration testing service to assess the security of your public-facing web application(s)** at least once a year.

WHY: Penetration testing helps you identify and plan to mitigate vulnerabilities. Though this can be costly and should be weighed against other budgetary considerations, web applications are an important area for penetration testing because they are the most public and vulnerable online systems for your organization.

HOW: Many cybersecurity companies offer penetration testing services. Use the questions in the Third Party section of this paper to evaluate potential vendors, and work with leadership to assess the viability of hiring such services.

Training Employees

Teach your employees accountability and strategies to minimize human error that could expose customer data.

WHY: Employees should feel responsible for customer data protection and follow clear policies when they handle sensitive information.

HOW: Advise and regularly train employees 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.

WHY: Employees should be fully trained on customer data protection policies so that they do not violate them, so they are fluent when dealing with customers, and so they do not communicate with customers in an unprotected manner.

HOW: Include customer data protection as a key component of employee training and include customer data security stipulations in your organization's cybersecurity policy.

Notifying Customers[116]

Understand your organization's **regulatory environment when it comes to handling customer data breaches.**

WHY: Having awareness of what will be required of your organization in case of an incident will ensure you are prepared to comply when incidents do occur.

HOW: Search for relevant regulations in your country, region, and internationally and record any requirements for which your organization will be responsible.[117] Your country's financial regulator may have resources to help better understand the regulatory environment.

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)** accordingly as soon as possible.

WHY: Promptly investigating unauthorized access to customer information is essential to determining whether the information has been or will be misused, and will inform how you must notify customers.

Many jurisdictions have customer notification requirements similar to the list below.

HOW: Following notification best practices, notify all customers as soon as possible following the incident 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.

Individual Advice for Customers and Employees to Protect Financial Data

Advise your employees and your customers to follow cybersecurity guidelines in their personal behavior.

WHY: Empowering customers and employees with cybersecurity best practices for their own behavior will increase their preparedness and help them protect their financial data from cyber threats.

HOW: Provide employees and customers, both through messaging and by making them publicly available, the following tips for protecting their financial data[118]:

1. Implement basic cyber hygiene practices across your devices.[119]
    - Use strong passwords and two-factor authentication on all personal and professional devices, and consider using a password manager.[120]
    - Keep operating systems and other software and applications up to date on your computers and mobile devices.[121]
    - Install anti-virus, anti-malware, and anti-ransomware software that prevents, detects and removes malicious programs.[122]
    - Use a firewall program to prevent unauthorized access to your computer.[123]
    - 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.[124]

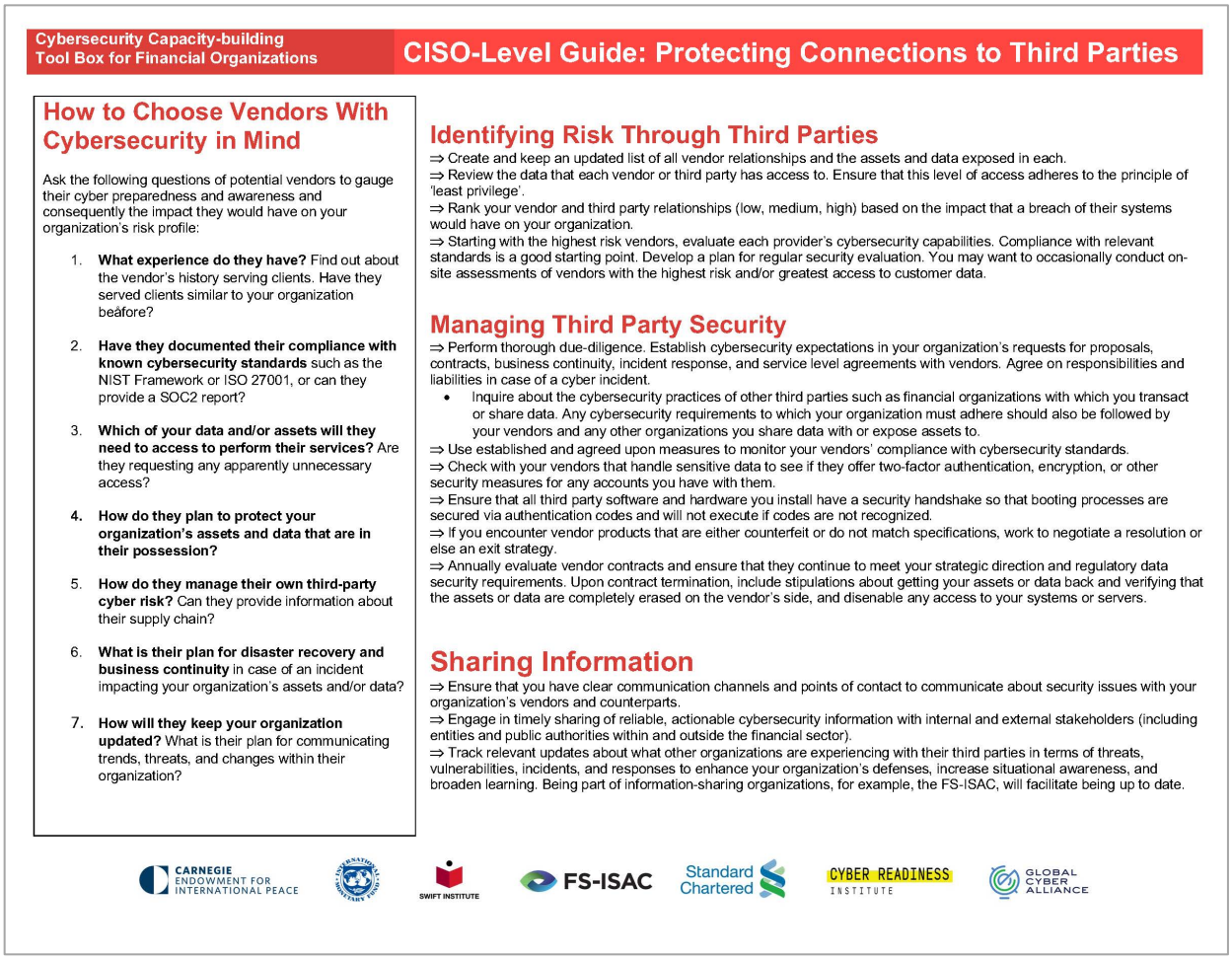
2. Be careful with sensitive information.
    - Do not send bank account passwords or other sensitive financial account data over unencrypted email.[125]
    - Be smart about where and how you connect to the Internet for banking or other communications involving sensitive personal information. Public Wi-Fi networks and computers at places such as libraries or hotel business centers are usually risky.[126]

3. Resist phishing.[127]
    - Don't immediately open email attachments or click on links in unsolicited or suspicious-looking emails. Stop. Think. Connect.[128]
    - 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.

5. IN DETAIL: "CISO-Level Guide: Protecting Connections to Third Parties"

Figure 6: CISO-Level Guide: Protecting Connections to Third Parties



A key feature of the financial system is the interconnectedness among the organizations that comprise it and between financial organizations and technology vendors. Many, if not most, of these relationships involve access and exchange of information, including sensitive customer data. The previous sections of this report have detailed how organizations should maintain robust cybersecurity for themselves. However, adhering to a standard of protection for your assets and data cannot be complete if you have opened up those possessions to vendors or third parties that you have not assessed or that you know to be less secure. The following section describes approaches your organization should take when evaluating potential vendors, as well as recommendations for managing the security of ongoing relationships with vendors and other third party organizations.

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?

WHY: Assessing a potential vendor's client experience will allow you to gauge whether they are equipped to fully and securely meet your needs.

HOW: As a first level of engagement with potential vendors you have selected, before drafting or signing any contracts or service agreements, ask a representative to explain and provide evidence of their experience serving clients similar to your organization. Have they worked with financial institutions and regulations? Have they worked with the kind of data and transactions you handle?

2. Have they documented their compliance with known cybersecurity standards?

WHY: If a vendor can demonstrate that they meet widely established, structured baselines, it will make it easier for you to understand whether their cybersecurity posture is a good fit for your organization.

HOW: During your initial engagement with the potential vendor, ask if they can provide documentation of their compliance with common cybersecurity standards such as the NIST Framework or ISO 27001 and/or if they have independent verifications such as a SOC2 report.[129]

3. Which of your data and/or assets will they need to access to perform their services?

WHY: Your organization has an understanding of the value and risks associated with each of its assets and types of data. Asking potential vendors how they will intersect with those elements will allow you to establish what additional risk you would take on when working with them and where that risk would be concentrated.

You should already be operating within your organization under the principle of least privilege, only providing employees and systems access to the assets and data they need to perform their functions. Assessing whether a potential vendor seems to be requesting access to assets or data that are not directly relevant to the tasks they will perform will allow you to

apply this principle to vendor management, preventing you from entering into any contracts or service agreements with potentially data-irresponsible organizations.

HOW: As discussions with a potential vendor progress and you have described the services your organization is seeking, ask the vendor to list which kinds of data and assets they will need to access to perform those services. You may provide them with a list of the types of assets and data your organization handles and ask them to justify each type of request for access. Ask follow-up questions where justifications are unclear.

4. How do they plan to protect your organization's assets and data that are in their possession?

WHY: Understanding a potential vendor's cybersecurity procedures is essential to moving forward with any arrangements. When they handle your assets and data, your vendors become a kind of extension of your own organization and must therefore meet your security needs and standards.

HOW: Ask for documentation of the potential vendor's cybersecurity, data management, and incident response plans and review them for any gaps between theirs and your own.

5. How do they manage their own third-party cyber risk? Can they provide information about their supply chain?

WHY: Just like your organization, your vendors likely need to rely on at least some third parties (eg., Cloud services, email providers) in their regular operations. This presents an additional layer of due diligence you should perform. The interconnectedness of technology dependencies means that supply chain risk assessments could hypothetically go on forever. However, do not allow this process to become an undue burden for your organization, but rather make judgements based on the level of risk involved about how far to pursue such assessments.

HOW: Ask the potential vendor whether they have asked this same (or comparable) list of questions to their own vendors. Require that they provide you with details of any third parties to which they will expose your organization's assets and data in the course of providing you services, including those parties' security compliance and points of contact.

6. What is their plan for disaster recovery and business continuity in case of an incident impacting your organization's assets and/or data?

WHY: As part of your own incident readiness, you should be aware of the notification and response practices in place among your vendors, whose incidents may become your own thanks to their possession of your data or connection to your assets.

HOW: Require that the potential vendor provide you with written copies of incident response and business continuity plans. Assess whether these are compatible with your own and appropriate to your regulatory environment and level of risk. Establish clear points of contact and responsibilities between your two organizations.

7. How will they keep your organization updated? What is their plan for communicating trends, threats, and changes within their organization?

WHY: Having a clear picture of your organization's cyber threat environment and security posture depends on having regular communication with vendors that interact with your data and assets.

HOW: Request documentation of the potential vendor's incident notification policies and agree on norms for regular information sharing. Ask what information sharing/threat intelligence networks they participate in/receive updates from.

Identifying Risk

Create and keep an updated list of all vendor relationships and the assets and data exposed in each.[130]

WHY: Having a holistic understanding of the location and status of your data and assets is the foundation of risk awareness and preparedness.

HOW: If you do not already keep such a list, write down all existing vendor relationships and the nature of the access involved for each. For each new vendor your organization hires, immediately add them to the list and record all access points. Update the list when any changes are made by you or your vendors.

Review the data to which 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 breach of their systems would have on your organization**.[131]

WHY: This will allow you to appropriately prioritize planning, protection, communication, and monitoring activities.

HOW: 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.[132]

The ranking of vendors, which are companies your organization formally contracts with to provide some service, should be based on the criticality your organization has established for the kinds of data and assets to which the vendor has access.

Third parties aside from vendors are any peer financial institutions or other organizations with which your organization shares sensitive data or to which access is granted to any assets. While you may not have the option in these relationships of instituting contractually mandated cybersecurity controls, you can and should make cybersecurity a part of your engagements with these third parties and come to mutual understanding of standards.

Starting with the highest risk vendors, **evaluate each provider's cybersecurity capabilities**.

WHY: With important data and assets exposed, your organization should extend its cybersecurity assessments to vendors to ensure holistic protection.

HOW: Compliance with relevant standards is a good starting point. Develop a plan for regular security evaluation.[133] You may want to occasionally conduct on-site assessments of the vendors with the highest risk and/or greatest access to customer data.[134]

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.

WHY: Any cybersecurity requirements to which your organization must adhere should ideally also be followed by your vendors and any other organizations you share data with or to which you expose assets.[135]

HOW: Use your organization's cybersecurity, data management, and incident response policies to inform the stipulations in agreements with vendors. Use established and agreed upon measures to monitor your vendors' compliance with cybersecurity standards.[136] Agree on responsibilities and liabilities in case of an 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.

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.[137]

WHY: Your organization should take advantage of all available security measures to ensure responsible data management between you and your vendors.

HOW: Check all default settings that come with the service, and enable any available tools (such as two-factor authentication via your email provider) to increase information security. Inquire with the vendor as to whether any further solutions are available.

Ensure that all third-party software and hardware you install have a **security handshake**.

WHY: This adds a layer of security to your organization's technology dependencies by ensuring that booting processes are secured via authentication codes and will not execute if codes are not recognized.[138]

HOW: Require a handshake in your contracts and double check with providers before installing software and hardware.[139]

If you encounter **vendor products that are either counterfeit or do not match specifications**, work to negotiate a resolution or else an exit strategy.[140]

WHY: Any security red flags must be resolved directly and with urgency, ideally by working with the vendor to resolve mistakes, but, in worst case, by terminating business with that vendor.

HOW: Notify the vendor as soon as possible and with as much detail as possible when you encounter such issues. The vendor's response (whether they are able to resolve the issue to your satisfaction) will determine whether you continue to contract with them.

Annually evaluate vendor contracts and ensure that they continue to meet your strategic direction and regulatory data security requirements.

WHY: Vendor security management is continuous and only ends when you can verify that the vendor no longer poses any risk to your organization through access to data or assets.

HOW: Include vendor contracts as part of your organization's overall cybersecurity review process. Contracts should include stipulations about getting your assets or data back and verifying that the assets or data are completely erased on the vendor's side when contracts are terminated.[141] Upon termination, disenable any access to your systems or servers by the vendor.

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.

WHY: With sensitive data and services flowing through your third-party relationships, regular communication between security personnel – as well as rapid notification in case of incidents – is crucial.

HOW: Ensure that points of contact are being maintained within your organization's master list of vendors and their access to data and assets. Ask the financial institutions and other organizations with which you transact to understand who to contact in case of emergency.

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).[142]

WHY: Voluntary information sharing builds a community of trust between organizations and within industries that enables collective monitoring and responsiveness to cyber threats.

HOW: Search for national and industry-based information sharing and collaboration programs such as your national CERT, the FS-ISAC, or other programs in your country or region.[143] These will provide a reporting, sharing, and learning structure for threat information. The U.S. NIST also offers a comprehensive guide on how to engage in cyber threat information sharing.[144]

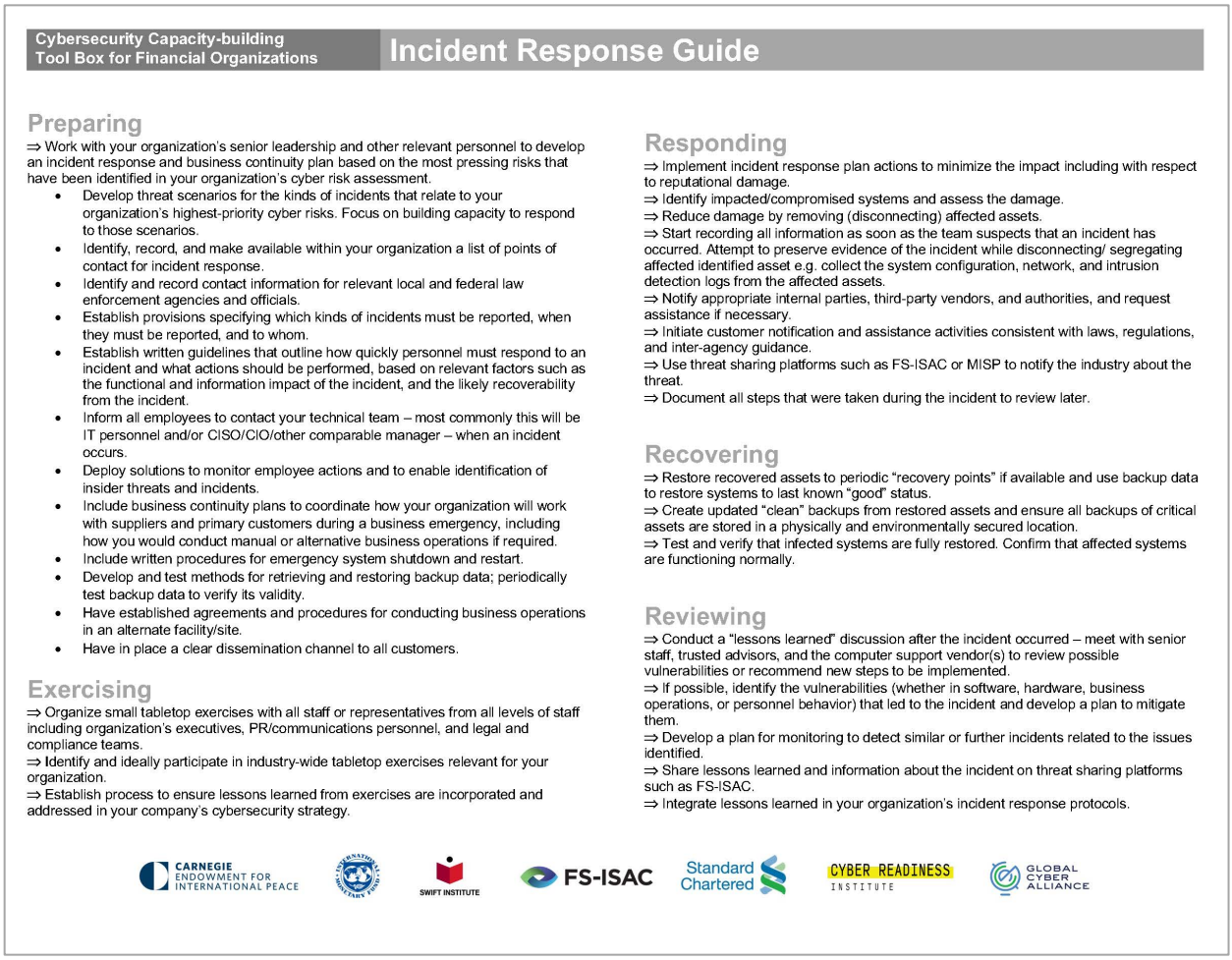
Track relevant updates about what other organizations are experiencing with their third parties in terms of threats, vulnerabilities, incidents, and responses.[145]

WHY: Staying up-to-date will enhance your organization's defenses, increase situational awareness, and broaden learning.

HOW: Being part of organizations like FS-ISAC or the US-CERT's free Automated Indicator Sharing (AIS) will give your organization a heads-up about such breaking stories.[146]

6. IN DETAIL: "Incident Response Guide"

Figure 7: Incident Response Guide



Many of the previous recommendations in this report focus on the first few pillars of cybersecurity management, "identify," "protect," and "detect." However, there has been a paradigm shift in cybersecurity circles in recent years away from a mode of prevention to a mode of resilience and incident response. This is the result of the deteriorating cybersecurity environment and a realization that even some of the most advanced and best-resourced organizations can be hacked. In other words, operating on the assumption that it is no longer a question 'if' but 'when' an organization will be hacked and preparing for the latter. Attention has therefore shifted away from assuming a cyber attack can be prevented 100% and toward a model that assumes an incident may happen eventually and trying to minimize its impact by developing an incident response plan. The focus on protecting against potential incidents therefore remains very important but has since been expanded to also focus on planning for how to respond and recover if an incident does happen. The following recommendations for incident response therefore cover the last pillars: "respond" and "recover."

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.

WHY: Cybersecurity awareness and capacity building can reduce the number of incidents your organization faces but cannot guarantee that all incidents will be prevented. Having carefully planned and recorded incident response capabilities is therefore necessary to enable your organization to react swiftly and properly in case of attack.

HOW: Consult detailed resources to guide you through the essential elements of an incident response plan.[147]

Develop threat scenarios for the kinds of incidents that relate to your organization's highest-priority cyber risks. Several organizations have published example scenarios and frameworks for threat profiling.[148] Focus your preparation and planning on building capacity to respond to those scenarios. Use guidelines about how to evaluate what is a critical incident and what is not.[149]

Establish provisions specifying which kinds of incidents must be reported, when they must be reported, and to whom.[150]

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.[151]

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. Have established agreements and procedures for conducting business operations in an alternate facility/site.[152]

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

WHY: Knowing in advance which law enforcement authorities, partners, and others must be contacted in case of an incident will reduce confusion and enable swift coordination.

HOW: Consult your national and regional regulations to identify what notification and/or communication steps may be required when cyber incidents occur. Confirm points of contact for cybersecurity coordination at each of your vendors and partner organizations. 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.

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. Technical personnel will then be responsible for communicating with external contacts.

Have in place a clear dissemination channel to all customers. This means having pre-written drafts of breach notification messages and having dedicated addresses and phone numbers for customers to contact you.

Ensure that your organization's executives, PR/communications personnel, legal and compliance teams, and vendors are **trained on incident response procedures**.[153]

WHY: Incident response is a whole-of-organization activity, beginning with understanding which personnel and assets have been affected to containing impacts to adjusting behavior and improving awareness post-incident. All personnel, not just technical staff, will need to have working familiarity with incident response plans for this process to be effective.

HOW: Ensure that your incident response plan is written out in accessible language and distributed to all staff, both through active trainings and in writing.

Deploy solutions to **monitor employee actions and correlate information** from multiple data sources.[154]

WHY: Responsible, deliberate employee monitoring will enable you to better identify insider threats and incidents and will help to map the development of many kinds of attacks.

HOW: Seek out features offered by your technology vendors such as email providers that allow you to monitor employee activity.[155] Be aware, however, that regulations such as Europe's General Data Protection Regulation (GDPR) place limits on employee monitoring.[156]

Develop and test methods for retrieving and restoring **backup data**; periodically test backup data to verify its validity. [157]

WHY: Keeping consistent backups will ease recovery after any cyber incidents affecting your data's availability or integrity.

HOW: Work with your backup storage provider(s), whether an outside vendor such as a Cloud service or your internal technical staff, to test the quality and usability of your organization's backups.

Exercising

Exercise your incident response plans in a variety of ways.

WHY: Having personnel across your organization practice your incident response plans will allow them to be executed successfully when a real incident occurs.

HOW: Organize small tabletop exercises with all staff or representatives from all levels of staff including 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.[158]

WHY: Planning turns to action when a cyber incident occurs.

HOW: Follow the steps laid out in your plan, including steps to

- Notify appropriate internal parties, third-party vendors, and authorities, request any necessary assistance,[159]

- Initiate customer notification and assistance activities consistent with laws, regulations, and inter-agency guidance;[160]
- 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.

Identify impacted/compromised systems and **assess the damage.**[161]

WHY: Responding to an incident often requires knowledge of what specifically occurred.

HOW: Know that attacks can occur along a variety of vectors. Be aware of common attack methods, listed by NIST as: external/removable media, brute force such as DDoS, cross site scripting attacks through the web, impersonation, improper usage, and loss or theft of equipment.[162]

Start with what brought the incident to your attention – what seems to be affected and/or malfunctioning? Who brought it to your attention? Look for common signs of attack, such as a suspiciously high volume of outgoing network traffic, increased disk activity, an auditing configuration change in a host's log, or suspicious files in the root directories of your drives.[163]

Work with your cybersecurity vendors, who will have more structured threat intelligence and incident information.

Remove/disconnect all affected assets.[164]

WHY: Isolating any assets that are compromised will reduce overall damage and allow you to focus on the issue at hand.

HOW: Remove all affected assets from your networks. Consult more detailed guides for complete containment and eradication steps.[165]

Start recording all information as soon as the team suspects that an incident has occurred.[166] Attempt to **preserve evidence of the incident** while disconnecting/ segregating affected identified assets.[167]

WHY: Keeping track of as much incident and handling information as possible will allow you to comply with law enforcement and support legal action. It will help your response process move forward in an organized manner and will enable you to conduct a review process later.

HOW: Consult your incident response plan, which should reference any laws and regulations that govern how you conduct your evidence gathering and preservation efforts.

Keep both paper and electronic records of the complete sequence of actions taken, including for each action the identifying information (the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer), the name, title, and contact information for each individual who collected or handled evidence, the time and date, and the locations where evidence was stored.[168]

Collect the system configuration, network, and intrusion detection logs from the affected assets.[169]

Recovering

Restore recovered assets to periodic "recovery points" if available and **use backup data to restore systems** to last known "good" status.[170]

WHY: Once assets are cleared of any issues, you can get back to regular business by using data and systems backups.

HOW: Follow instructions from your data storage provider. Remember that updating recovered systems with current data may require you to manually input transactions if business was conducted offline due to the cyber event.

Create updated "clean" backups from restored assets and ensure all backups of critical assets are stored in a physically and environmentally secured location.[171]

WHY: Keeping up-to-date, secured, malware-free backups allows you to recover again in the future.

HOW: Take this step after containing, eradicating, and analyzing the incident that occurred. Work with your data storage provider(s) to update and secure a new, full backup of your systems and data.

Test and verify that **infected systems are fully restored**. Confirm that affected systems are functioning normally.[172]

WHY: Full recovery from an incident occurs when all systems are functioning properly to support regular operations.

HOW: Technical staff should have clear understanding of the normal behaviors of your networks, systems, and applications. Work with your team to run tests, monitor logs, and handle any continuing issues.[173]

Reviewing

Conduct a "lessons learned" discussion after the incident occurred.

WHY: Reviewing the incident and the effectiveness of your organization's response is a crucial step to ensure that each incident is an opportunity to improve security. All key personnel involved in incident response must reflect on their role to help improve the process moving forward.

HOW: Meet with senior staff, trusted advisors, and the computer support vendor(s) to review the entire incident response process.[174] Use the detailed records you kept during the response process to guide discussion.

Develop an action plan to leverage lessons learned, including both technical and non-technical steps. If possible, identify any gaps or vulnerabilities (whether in software, hardware, business operations, or personnel behavior) that led to the incident and develop a plan to mitigate them.[175] Develop a plan for monitoring to detect similar or further incidents related to the issues identified.[176] Assign each step to specific individuals or teams and

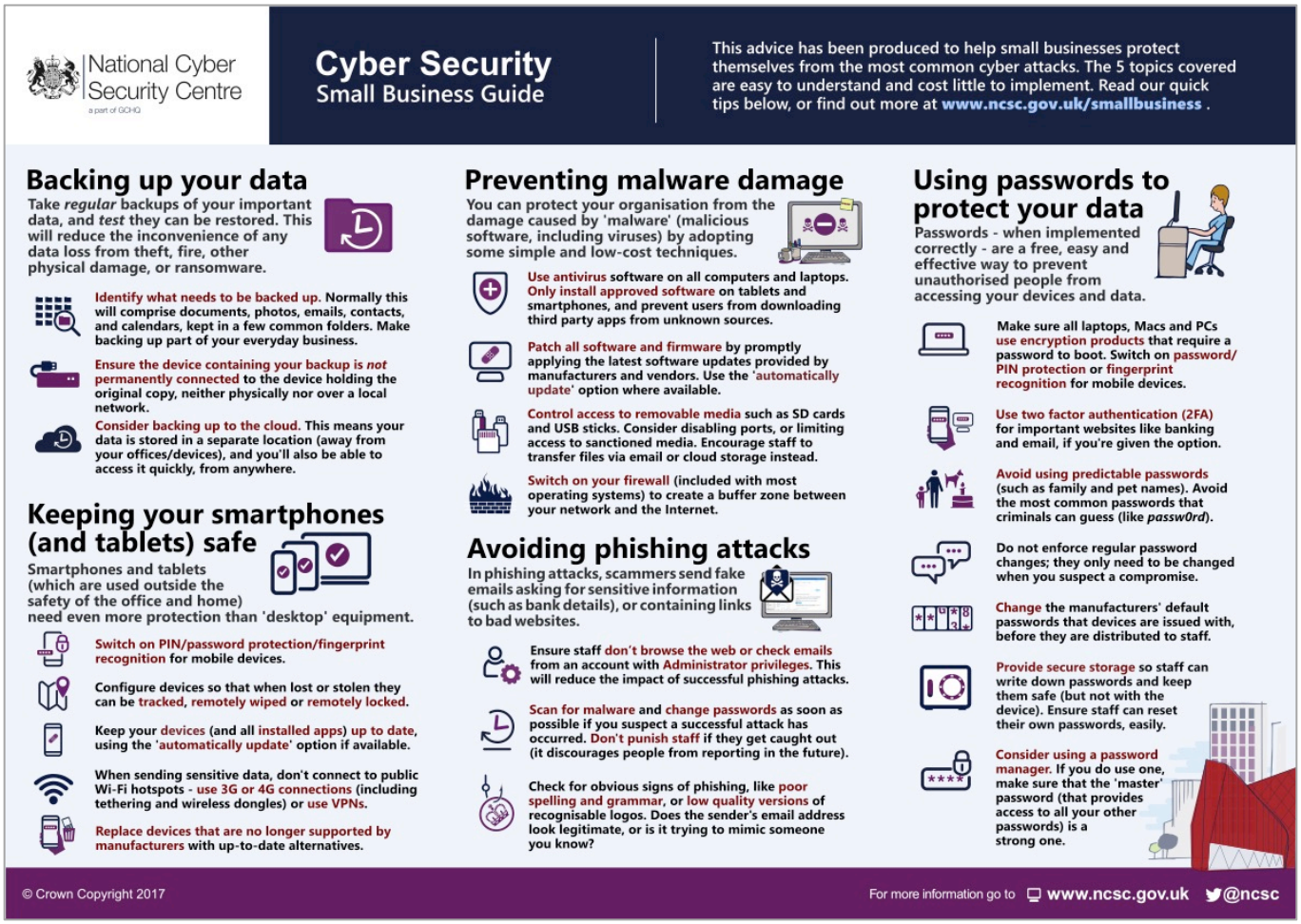
establish clear goals and check-ins.[177] Make a plan to conduct an exercise of you organization's incident response protocols.

Share the lessons learned and information about the incident on threat sharing platform such as FS-ISAC. Integrate lessons learned in your organization's incident response protocols.

Appendix

At the beginning of this project, we decided to focus on developing a series of actionable one-page guides and checklists in addition to a detailed supplementary report. Following our initial desk research, we found the UK NCSC Cybersecurity Small Business Guide to be a useful template for this purpose but expanded it to also capture (a) the critical role of CEOs and an organization's board and (b) to capture the different dimensions of a CISO's responsibilities and focus – own organization, customers, and third parties.[178]

Figure 8: Cybersecurity Small Business Guide



References

1. "A Bank Customer's Guide to Cybersecurity," FDIC Consumer News, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf.
2. Andrew Morris, "Catching Up with the ACET," NAFCU Compliance Blog, March 19, 2018, https://nafcucomplianceblog.typepad.com/nafcu_weblog/2018/03/catching-up-with-the-acet.html.
3. Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," IMF Working Papers, June 22, 2018, https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.
4. Aquiles A. Almansi, Yejin Carol Lee, and Jiemin Ren, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, August 2018, http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf.
5. "Assessments: Cyber Resilience Review (CRR)," United States Computer Emergency Readiness Team, https://www.us-cert.gov/ccubedvp/assessments.
6. "Authentication in an Internet Banking Environment," Federal Financial Institutions Examination Council, June 28, 2011, https://www.ffiec.gov/pdf/authentication_guidance.pdf.
7. Ben Rogers, "3 Cybersecurity Threats Facing Credit Unions," Credit Union Times, June 16, 2016, https://www.cutimes.com/2016/06/16/3-cybersecurity-threats-facing-credit-unions/?slreturn=20181020112243.
8. Celia Paulsen and Patricia Toth, "Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.
9. "CIS Controls: Implementation Guide for Small- and Medium-Sized Enterprises (SMEs)," Center for Internet Security, September 14, 2017, https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf.
10. Craig Nazzaro, "Best Practices in Data Security for Financial Institutions," January 2017, http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/01/01/best-practices-in-data-security-for-financial-institutions/?slreturn=20181020111138.
11. "Customer Security Programme (CSP)," SWIFT, https://www.swift.com/myswift/customer-security-programme-csp.
12. "Cyber Lexicon: Consultative Document," Financial Stability Board, July 2, 2018, http://www.fsb.org/wp-content/uploads/P020718.pdf.
13. "Cybersecurity 101: A Resource Guide for Bank Executives," Conference of State Bank Supervisors, November 2017, https://www.csbs.org/sites/default/files/2017-11/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf.

14. "Cybersecurity Assessment Tool," Federal Financial Institutions Examination Council, May 2017, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.
15. "Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Board Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf.
16. "Cybersecurity: Credit Unions in the Crosshairs," Filene Research Institute, May 31, 2016, https://filene.org/learn-something/reports/cybersecurity-credit-unions-in-the-crosshairs.
17. "Cybersecurity for Small Business," U.S. Federal Communications Commission, https://www.fcc.gov/general/cybersecurity-small-business.
18. "Cyber Security Resources," National Credit Union Administration, https://www.ncua.gov/regulation-supervision/Pages/policy-compliance/resource-centers/cyber-security.aspx.
19. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," Official Journal of the European Union, July 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.
20. Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, "Cyber Risk, Market Failures, and Financial Stability," IMF Working Papers, August 7, 2017, https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104.
21. "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, October 2017, http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf.
22. "Financial Services Sector Cybersecurity Profile," Financial Services Sector Coordinating Council, https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile.
23. "Focus: Banks and Cyber Security," Canadian Bankers Association, September 18, 2018, https://cba.ca/banks-and-cyber-security.
24. "Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1," National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
25. Frankie E Catota, M Granger Morgan, and Douglas C Sicker, "Cybersecurity incident response capabilities in the Ecuadorian financial sector," Journal of Cybersecurity, April 30, 2018, https://academic.oup.com/cybersecurity/advance-article/doi/10.1093/cybsec/tyy002/4990518.
26. "FS-ISAC Unveils 2018 Cybersecurity Trends According to Top Financial CISOs," Financial Services Information Sharing and Analysis Center, February 12, 2018,

https://www.fsisac.com/article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos.
27. "G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector," G7, October 20, 2017, http://www.mef.gov.it/inevidenza/documenti/PRA_BCV_4728453_v_1_G7_Fundamental.pdf.
28. "G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector," G7, October 15, 2018, https://fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf.
29. "G7 Fundamental Elements of Cybersecurity for the Financial Sector," G7, October 2016, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf.
30. "Global financial services third-party risk management survey," Ernst & Young, 2018, https://www.ey.com/Publication/vwLUAssets/ey-global-financial-services-third-party-risk-management-survey/%24File/ey-global-financial-services-third-party-risk-management-survey.pdf.
31. Harold Gallagher, Wade McMahon, and Ron Morrow, "Cyber Security: Protecting the Resilience of Canada's Financial System," Bank of Canada Financial System Review, December 2014, https://www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf.
32. "ISO/IEC 27000 family – Information security management systems," International Organization for Standardization, https://www.iso.org/isoiec-27001-information-security.html.
33. Melissa Stevens, "Vendor Risk Management: What Increases Your Risk & How To Combat It," BitSight, July 18, 2017, https://www.bitsighttech.com/blog/vendor-risk-management-principles.
34. Nick Price, "Cybersecurity Best Practices for Credit Unions," Board Effect, June 29, 2018, https://boardeffect.com/blog/cybersecurity-best-practices-credit-unions/.
35. "NIST Small Business Cybersecurity Act," 115th Congress, January 3, 2018, https://www.gpo.gov/fdsys/pkg/BILLS-115s770enr/pdf/BILLS-115s770enr.pdf.
36. "Observations from Cybersecurity Examinations," Office of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission, August 7, 2017, https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.
37. "Report on Cyber Security in the Banking Sector," New York State Department of Financial Services, May 2014, https://www.dfs.ny.gov/reportpub/cyber/dfs_cyber_banking_report_052014.pdf.
38. "Small Business Tip Card," U.S. Department of Homeland Security, April 2007, https://www.dhs.gov/sites/default/files/publications/Small%20Business%20Tip%20Card_0.pdf.

39. "Small Firms Cybersecurity Guidance: How to Consume Threat Information from the FS-ISAC," Securities Industry and Financial Markets Association, 2017, https://www.sifma.org/wp-content/uploads/2017/07/small-firms-cybersecurity-guide-2017.pdf.
40. "SOC 2® - SOC for Service Organizations: Trust Services Criteria," American Institute of Certified Public Accountants, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html.
41. "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices," Financial Stability Board, October 13, 2017, http://www.fsb.org/wp-content/uploads/P131017-2.pdf.
42. "Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices," Financial Stability Board, October 13, 2017, http://www.fsb.org/wp-content/uploads/P131017-1.pdf.
43. "The Ethics of Data Sharing: A guide to best practices and governance," Accenture Labs, November 10, 2016, https://www.accenture.com/t20161110T001618Z__w__/us-en/_acnmedia/PDF-35/Accenture-The-Ethics-of-Data-Sharing.pdf#zoom=50.
44. "Tips for Financial Institutions: What to do Post-Breach," Financial Services Information Sharing and Analysis Center, September 21, 2017, https://www.fsisac.com/sites/default/files/news/FSISAC_Tips_for_FinInstutions-WhatToDoPostBreach-TLPWhite-FIN.pdf.

Notes

[1] G20 Finance Ministers and Central Bank Governors Communiqué, Baden Baden, March 18, 2017, http://www.g20.utoronto.ca/2017/170318-finance-en.html.

[2] "FSB publishes stocktake on cybersecurity regulatory and supervisory practices," Financial Stability Board, October 13, 2017, http://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/; Christine Lagarde, "Estimating Cyber Risk for the Financial Sector," IMFBlog, June 22, 2018, https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/; "Guidance on cyber resilience for financial market infrastructures," CPMI-IOSCO, June 2016, https://www.bis.org/cpmi/publ/d146.pdf; Komal Gupta, "Govt working to set up financial CERT to tackle cyber threats," Livemint, November 16, 2017, https://www.livemint.com/Industry/KMK5eQsbcJpYvEMPfp5MHI/Govt-working-to-set-up-financial-CERT-to-tackle-cyber-threat.html; "Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union," Official Journal of the European Union, July 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN; "Technology Risk Management Guidelines," Monetary Authority of Singapore, June 2013, http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf; Claudia Chong and Ng Jun Sen, "MAS plans 6 cyber security rules for financial institutions," *Straits Times*, September 7, 2018, https://www.straitstimes.com/business/mas-plans-6-cyber-security-rules-for-financial-institutions; "FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC)," FS-ISAC, October 24, 2016, https://www.fsisac.com/sites/default/files/news/FS-ISAC%20Announces%20the%20Formation%20of%20the%20Financial%20Systemic%20Analysis%20(FSARC).pdf.

[3] Rick Gladstone, "Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million," New York Times, March 15, 2016, https://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html?_r=0.

[4] "2018 Data Breach Investigations Report," Verizon, March 2018, https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

[5] Roy Urrico, "Malware Attacks Targeting Smaller Financial Institutions," Credit Union Times, July 20, 2016, https://www.cutimes.com/2016/07/20/malware-attacks-targeting-smaller-financial-instit/.

[6] For more details, see Carnegie's 'Timeline of Cyber Incidents involving Financial Institutions' available at www.carnegieendowment.org/fincyber/

[7] "Mexico central bank to create cyber security unit after hack," Reuters, May 15, 2018, https://www.reuters.com/article/us-mexico-cyber/mexico-central-bank-to-create-cyber-security-unit-after-hack-idUSKCN1IG3AB.

[8] "G7 fundamental elements of cybersecurity in the financial sector," European Commission, October 11, 2016, https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en.

[9] Documents included in the analysis range from general guidance such as the NIST Cybersecurity Framework and the EU's NIS Directive to specific guidance for the financial industry, such as SWIFT's Customer Security Program, CPMI-IOSCO's guidance on cyber resilience for financial market infrastructures, and the FFIEC's Cybersecurity Assessment Tool to specific guidance for small businesses, including documents published by the UK's NCSC and the U.S.'s FCC, FTC, and NIST

[10] It is important here to highlight specifically that, while there is growing consensus on the security benefits smaller organizations can gain from migrating to the Cloud, policies remain evolving. We

encourage organizations to explore migrating to the Cloud while tracking near- and mid-term policy developments. Our section on Protecting Connections to Third Parties offers more guidance on how to evaluate potential third-party technology providers.

11 TheCityUK and Marsh produced this list of fundamental questions for boards to govern cyber risk: "Governing Cyber Risk: A Guide for Company Boards," TheCityUK and Marsh, April 2018, https://www.marsh.com/uk/insights/research/governing-cyber-risk-a-guide-for-company-boards.html.

12 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

13 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

14 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

15 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

16 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

17 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf; "FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf.

18 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

19 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

20 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf; "Guidance on cyber resilience for financial market infrastructures," CPMI-IOSCO, June 2016, https://www.bis.org/cpmi/publ/d146.pdf.

21 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

22 "Governing Cyber Risk: A Guide for Company Boards," TheCityUK and Marsh, April 2018, https://www.marsh.com/uk/insights/research/governing-cyber-risk-a-guide-for-company-boards.html.

23 "Advancing Cyber Resilience: Principles and Tools for Boards," World Economic Forum, January 2017, http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf.

24 "Governing Cyber Risk: A Guide for Company Boards," TheCityUK and Marsh, April 2018, https://www.marsh.com/uk/insights/research/governing-cyber-risk-a-guide-for-company-boards.html.

25 "Governing Cyber Risk: A Guide for Company Boards," TheCityUK and Marsh, April 2018, https://www.marsh.com/uk/insights/research/governing-cyber-risk-a-guide-for-company-boards.html.

26 "Governing Cyber Risk: A Guide for Company Boards," TheCityUK and Marsh, April 2018, https://www.marsh.com/uk/insights/research/governing-cyber-risk-a-guide-for-company-boards.html.

27 "Governing Cyber Risk: A Guide for Company Boards," TheCityUK and Marsh, April 2018, https://www.marsh.com/uk/insights/research/governing-cyber-risk-a-guide-for-company-boards.html.

28 "Governing Cyber Risk: A Guide for Company Boards," TheCityUK and Marsh, April 2018, https://www.marsh.com/uk/insights/research/governing-cyber-risk-a-guide-for-company-boards.html.

29 "Guidance on cyber resilience for financial market infrastructures," CPMI-IOSCO, June 2016, https://www.bis.org/cpmi/publ/d146.pdf.

[30] "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture," Financial Stability Board, April 7, 2014, http://www.fsb.org/wp-content/uploads/140407.pdf

[31] "Guidance on cyber resilience for financial market infrastructures," CPMI-IOSCO, June 2016, https://www.bis.org/cpmi/publ/d146.pdf.

[32] "Guidance on cyber resilience for financial market infrastructures," CPMI-IOSCO, June 2016, https://www.bis.org/cpmi/publ/d146.pdf.

[33] CPMI-IOSCO offers guidance for boards and senior leadership on effective cybersecurity governance: "Guidance on cyber resilience for financial market infrastructures," CPMI-IOSCO, June 2016, https://www.bis.org/cpmi/publ/d146.pdf.

[34] "Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organizations managing ICT operations," Indian-Computer Emergency Response Team, Ministry of Electronics and IT, Government of India, March 14, 2017, http://meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf.

[35] "Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organizations managing ICT operations," Indian-Computer Emergency Response Team, Ministry of Electronics and IT, Government of India, March 14, 2017, http://meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf, pages 2-6; Dejan Kosutic, "What is the job of Chief Information Security Office (CISO) in ISO 27001?" ISO 27001 and ISO 22301 Consultation Center, https://advisera.com/27001academy/knowledgebase/what-is-the-job-of-chief-information-security-officer-ciso-in-iso-27001/.

[36] "Fundamental Elements of Cybersecurity for the Financial Sector," G7, October 11, 2016, https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf.

[37] "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices," Financial Stability Board, October 13, 2017, http://www.fsb.org/wp-content/uploads/P131017-2.pdf; Aquiles A. Almansi, Yejin Carol Lee, and Jiemin Ren, "Financial Sector's Cybersecurity: A Regulatory Digest," World Bank Group, August 2018, http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf.

[38] "FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf; "Financial Services Sector Cybersecurity Profile," Financial Services Sector Coordinating Council, https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile.

[39] Celia Paulsen and Patricia Toth, "Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

[40] "Fundamental Elements of Cybersecurity for the Financial Sector," G7, October 11, 2016, https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf.

[41] Craig Nazzaro, "Best Practices in Data Security for Financial Institutions," *Law Journal Newsletters*, January 2017, http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/01/01/best-practices-in-data-security-for-financial-institutions/.

[42] The FSB describes foundational elements of sound risk culture and provides guidance for boards and senior management to govern and set the tone in their organizations' cybersecurity: "Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture," Financial Stability Board, April 7, 2014, http://www.fsb.org/wp-content/uploads/140407.pdf.

The German Federal Office for Information Security also offers a guide for managers to understand, plan, and optimize information security: "IT-Grundschutz: An Overview: Decision Guide for Managers," German Federal Office for Information Security, April 2013, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/IT-Grundschutz_Guide_for_Managers.pdf?__blob=publicationFile&v=1. See also: Dejan Kosutic, "Risk assessment tips for smaller companies," ISO 27001 and ISO 22301 Blog, February 22, 2010, https://advisera.com/27001academy/blog/2010/02/22/risk-assessment-tips-for-smaller-companies/?icn=free-blog-27001&ici=top-risk-assessment-tips-for-smaller-companies-txt.

43 "IT-Grundschutz An Overview: Decision Guide for Managers," Bundesamt für Sicherheit in der Informationstechnik, April 2013, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/IT-Grundschutz_Guide_for_Managers.pdf?__blob=publicationFile&v=1.

44 "FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf; "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

45 "FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf.

46 "FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf.

47 "FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf.

48 "FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors," Federal Financial Institutions Examination Council, June 2015, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf.

49 "C3 Voluntary Program Cyber Risk Management Primer for CEOs," U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf.

50 Craig Nazzaro, "Best Practices in Data Security for Financial Institutions," *Law Journal Newsletters*, January 2017, http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/01/01/best-practices-in-data-security-for-financial-institutions/.

51 "Information Sharing Resources," Investment Company Institute, https://www.ici.org/info_security/sharing; "Cybersecurity Resource Guide for Financial Institutions," FFIEC, October 2018, https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf; Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/; "Cyber Information Sharing and Collaboration Program (CISCP)," U.S. Department of Homeland Security, September 25, 2018, https://www.dhs.gov/ciscp.

52 For more information about FS-ISAC's functions and services, see "Testimony of Bill Nelson, President and CEO of the Financial Services Information Sharing and Analysis Center (FS-ISAC)," Committee on Banking, Housing and Urban Affairs, U.S. Senate, May 24, 2018, https://www.fsisac.com/sites/default/files/news/FSISAC-NelsonTestimony_20180524.pdf.

53 Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, and Clem Skorupka, "Guide to Cyber Threat Information Sharing," National Institute of Standards and Technology, October 2016, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf.

[54] NIST's guide for small businesses is a helpful application of the approaches outlined in the NIST Framework to the specific situation of smaller organizations: Celia Paulsen and Patricia Toth, "Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf. Other helpful frameworks to consult when developing your information security program and policies: "Cybersecurity Assessment Tool," FFIEC, June 2015, https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_june_2015_pdf2.pdf; "Fundamental Elements of Cybersecurity for the Financial Sector," G7, October 11, 2016, https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf; Dejan Kosutic, "ISO 27001 implementation checklist," ISO 27001/ISO 22301 Knowledge Base, https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/.

[55] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/know-what-you-have/.

[56] "Information Sharing Resources," Investment Company Institute, https://www.ici.org/info_security/sharing; "Cybersecurity Resource Guide for Financial Institutions," FFIEC, October 2018, https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf; Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/.

[57] "Fundamental Elements of Cybersecurity for the Financial Sector," G7, October 11, 2016, https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf.

[58] For example, in the European context ("Final Report: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)," European Banking Authority, May 11, 2017, https://eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a) and in Singapore ("Technology Risk Management Guidelines," Monetary Authority of Singapore, June 2013, http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf).

[59] "Cyber Security Small Business Guide," National Cyber Security Centre, October 11, 2017, https://www.ncsc.gov.uk/collection/small-business-guide?curPage=/collection/small-business-guide/cyber-security-small-business-guide-infographic.

[60] Eric Vasbinder, "How to make the most of access control lists," Computer World, November 20, 2003, https://www.computerworld.com/article/2573380/security0/how-to-make-the-most-of-access-control-lists.html.

[61] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/prevent-phishing-and-viruses/.

[62] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/update-your-defenses/.

[63] Celia Paulsen and Patricia Toth, "Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[64] Karen Kent and Murugiah Souppaya, "Guide to Computer Security Log Management," National Institute of Standards and Technology, September 2006, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf.

[65] Karen Kent and Murugiah Souppaya, "Guide to Computer Security Log Management," National Institute of Standards and Technology, September 2006, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf; John Creasey, "Cyber Security Monitoring and Logging Guide," CREST, 2015, https://www.crest-approved.org/wp-

content/uploads/2015/05/Cyber-Security-Monitoring-Guide.pdf; "Effective Log Management," UK Centre for the Protection of National Infrastructure, May 7, 2014, https://www.ncsc.gov.uk/content/files/protected_files/document_files/2014-05-07-Effective%20Log%20Management%20Booklet.pdf.

66 Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology," National Institute of Standards and Technology, 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

67 Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf; "NTP: The Network Time Protocol," http://www.ntp.org/.

68 The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/know-what-you-have/.

69 The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/protect-your-brand/.

70 "Small Business Tip Card," U.S. Department of Homeland Security, April 2007, https://www.dhs.gov/sites/default/files/publications/Small%20Business%20Tip%20Card_0.pdf.

71 The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/.

72 "Cyber Security Small Business Guide," National Cyber Security Centre, October 11, 2017, https://www.ncsc.gov.uk/collection/small-business-guide?curPage=/collection/small-business-guide/cyber-security-small-business-guide-infographic.

73 The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/defend-against-ransomware/.

74 Paul Mah, "How to Build a Storage and Backup Strategy for Your Small Business, CIO, March 11, 2014 https://www.cio.com/article/2378019/small-business/how-to-build-a-storage-and-backup-strategy-for-your-small-business.html.

75 NIST offers helpful definitions of Cloud computing and its characteristics: "NIST Cloud Computing Standards Roadmap," National Institute of Standards and Technology, July 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf, pages 8-10. Also see "Cloud Computing Service Metrics Description," National Institute of Standards and Technology, 2015, https://www.nist.gov/sites/default/files/documents/itl/cloud/RATAX-CloudServiceMetricsDescription-DRAFT-20141111.pdf; "Recommendations for companies planning to use Cloud computing services," French data protection authority, June 25, 2012, https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf; "Ten Questions to Ask Your Cloud Vendor Before Entering the Cloud," Oracle, May 2012, http://www.oracle.com/us/products/applications/10-questions-for-cloud-vendors-1639601.pdf; Mary Shacklett, "The top cloud providers for financial services," ZDNet, April 1, 2015, https://www.zdnet.com/article/the-top-cloud-providers-for-financial-services/.

76 Celia Paulsen and Patricia Toth, "Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

77 "Cyber Security Small Business Guide," National Cyber Security Centre, October 11, 2017, https://www.ncsc.gov.uk/collection/small-business-guide?curPage=/collection/small-business-guide/cyber-security-small-business-guide-infographic.

[78] "Find My iPhone," Apple, https://support.apple.com/explore/find-my-iphone-ipad-mac-watch; "Find, lock, or erase a lost Android device," Google, https://support.google.com/android/answer/6160491?hl=en.

[79] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/update-your-defenses/.

[80] "Cyber Security Small Business Guide," National Cyber Security Centre, October 11, 2017, https://www.ncsc.gov.uk/collection/small-business-guide?curPage=/collection/small-business-guide/cyber-security-small-business-guide-infographic.

[81] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/.

[82] John Hall, "SplashData's Top 100 Worst Passwords of 2018," https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/.

[83] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, "Digital Identity Guidelines," National Institute of Standards and Technology, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf; Jim Fenton, "Toward Better Password Requirements," August 2, 2016, https://www.slideshare.net/jim_fenton/toward-better-password-requirements; "Create a strong password & a more secure account," Google, https://support.google.com/accounts/answer/32040?hl=en.

[84] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/.

[85] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/beyond-simple-passwords.

[86] "1Password Business," https://1password.com/business/; "Business Password Manager," LastPass, https://www.lastpass.com/business-password-manager.

[87] "Ten Cybersecurity Tips for Small Businesses," Federal Communications Commission, May 16, 2011, https://www.fcc.gov/document/ten-cybersecurity-tips-small-businesses.

[88] "Australian Government Information Security Manual Controls," Australian Department of Defence, September 29, 2017, https://acsc.gov.au/publications/Information_Security_Manual_2017_Controls.pdf.

[89] "Network security – the basics," UK Financial Conduct Authority, 2018, https://www.fca.org.uk/publication/systems-information/network-security-basics.pdf.

[90] "Ten Cybersecurity Tips for Small Businesses," Federal Communications Commission, May 16, 2011, https://www.fcc.gov/document/ten-cybersecurity-tips-small-businesses.

[91] "Security Tip (ST05-003): Securing Wireless Networks," US-CERT, March 11, 2010, https://www.us-cert.gov/ncas/tips/ST05-003.

[92] "Small Business Computer Security Basics," Federal Trade Commission, April 2017, https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics.

[93] "Setting your WiFi encryption as WPA2-PSK," Enplug Support Center, https://support.enplug.com/hc/en-us/articles/205160175-Setting-your-WiFi-encryption-as-WPA2-PSK.

[94] "Small Business Computer Security Basics," Federal Trade Commission, April 2017, https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics.

[95] "Small Business Computer Security Basics," Federal Trade Commission, April 2017, https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics.

[96] "Ten Cybersecurity Tips for Small Businesses," Federal Communications Commission, May 16, 2011, https://www.fcc.gov/document/ten-cybersecurity-tips-small-businesses.

[97] "Small Business Computer Security Basics," Federal Trade Commission, April 2017, https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics.

[98] "CIS Controls Implementation Guide for SMEs," Center for Internet Security, September 2017, https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf.

[99] "Small Business Computer Security Basics," Federal Trade Commission, April 2017, https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics.
[100] "Small Business Computer Security Basics," Federal Trade Commission, April 2017, https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics.
[101] "Cyber Security Small Business Guide," National Cyber Security Centre, October 11, 2017, https://www.ncsc.gov.uk/collection/small-business-guide?curPage=/collection/small-business-guide/cyber-security-small-business-guide-infographic.
[102] Celia Paulsen and Patricia Toth, "Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf; The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/protect-your-brand/.
[103] Celia Paulsen and Patricia Toth, "Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.
[104] "Phishing," Microsoft, August 16, 2018, https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing.
[105] "How to Run a Phishing Test on Your Employees," Infosec Institute, July 26, 2018, https://resources.infosecinstitute.com/how-to-run-a-phishing-test-on-your-employees/.
[106] "Tips for Financial Institutions: What to do Post-Breach," Financial Services Information Sharing and Analysis Center, September 21, 2017, https://www.fsisac.com/sites/default/files/news/FSISAC_Tips_for_FinInstutions-WhatToDoPostBreach-TLPWhite-FIN.pdf.
[107] "A Bank Customer's Guide to Cybersecurity," *FDIC Consumer News*, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf.
[108] "Best Practices for Fraud Prevention," Bank of America Merrill Lynch, 2015, http://corp.bankofamerica.com/documents/10157/67594/Best_Practices_for_Fraud_Prevention.pdf
[109] "Building digital trust: The role of data ethics in the digital age," Accenture Labs, June 13, 2016, https://www.accenture.com/t20180705T112503Z__w__/us-en/_acnmedia/PDF-22/Accenture-Data-Ethics-POV-WEB.pdf#zoom=50.
[110] For example, Microsoft Azure offers a guide to using encryption for data security: "Azure Data Security and Encryption Best Practices," Microsoft, December 18, 2018, https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices.
[111] Rob Griffith, "5 Cybersecurity Solutions To Benefit Your Bank," Aureon, October 23, 2017, https://www.aureon.com/blog/5-cybersecurity-solutions-to-benefit-your-bank.
[112] Brian Jackson, "Complete Guide – How to Migrate from HTTP to HTTPS," KeyCDN, January 23, 2018, https://www.keycdn.com/blog/http-to-https.
[113] "Content Security Policy (CSP)," MDN web docs, August 24, 2018, https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP; Mike West and Joseph Medley, "Content Security Policy," Google Web Fundamentals, September 21, 2018, https://developers.google.com/web/fundamentals/security/csp/; Cody Arsenault, "11 Web Application Security Best Practices," KeyCDN, January 9, 2017, https://www.keycdn.com/blog/web-application-security-best-practices.
[114] "HTTP Public Key Pinning (HPKP)," MDN web docs, November 13, 2018, https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning; Cody Arsenault, "11 Web Application Security Best Practices," KeyCDN, January 9, 2017, https://www.keycdn.com/blog/web-application-security-best-practices.
[115] Cody Arsenault, "11 Web Application Security Best Practices," KeyCDN, January 9, 2017, https://www.keycdn.com/blog/web-application-security-best-practices.

[116] "Tips for Financial Institutions: What to do Post-Breach," Financial Services Information Sharing and Analysis Center, September 21, 2017, https://www.fsisac.com/sites/default/files/news/FSISAC_Tips_for_FinInstutions-WhatToDoPostBreach-TLPWhite-FIN.pdf.

[117] "Compare data protection laws around the world," DLA Piper, 2018, https://www.dlapiperdataprotection.com/.

[118] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org.

[119] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/prevent-phishing-and-viruses/.

[120] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/.

[121] The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/update-your-defenses/.

[122] A Bank Customer's Guide to Cybersecurity," *FDIC Consumer News*, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf; The GCA Cybersecurity Toolkit for Small Business offers useful additional resources on this topic here: https://gcatoolkit.org/smallbusiness/prevent-phishing-and-viruses/.

[123] A Bank Customer's Guide to Cybersecurity," *FDIC Consumer News*, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf.

[124] A Bank Customer's Guide to Cybersecurity," *FDIC Consumer News*, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf.

[125] A Bank Customer's Guide to Cybersecurity," *FDIC Consumer News*, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf.

[126] A Bank Customer's Guide to Cybersecurity," *FDIC Consumer News*, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf.

[127] A Bank Customer's Guide to Cybersecurity," *FDIC Consumer News*, Winter 2016, https://www.bankfcb.com/pdfs/FDIC_news.pdf.

[128] For more details on the 'Stop. Think. Connect' awareness-raising campaign, visit: www.stopthinkconnect.org

[129] "Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework; "ISO/IEC 27000 family – Information security management systems," International Organization for Standardization, https://www.iso.org/isoiec-27001-information-security.html; "SOC 2® - SOC for Service Organizations: Trust Services Criteria," American Institute of Certified Public Accountants, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html.

[130] Aaron Wooten, "Third-Party Cyber Security: Strengthening the Weak Link," CSO Australia, July 2, 2018, https://www.cso.com.au/article/643238/third-party-cyber-security-strengthening-weak-link/.

[131] Aaron Wooten, "Third-Party Cyber Security: Strengthening the Weak Link," CSO Australia, July 2, 2018, https://www.cso.com.au/article/643238/third-party-cyber-security-strengthening-weak-link/.

[132] Aaron Wooten, "Third-Party Cyber Security: Strengthening the Weak Link," CSO Australia, July 2, 2018, https://www.cso.com.au/article/643238/third-party-cyber-security-strengthening-weak-link/.

[133] Aaron Wooten, "Third-Party Cyber Security: Strengthening the Weak Link," CSO Australia, July 2, 2018, https://www.cso.com.au/article/643238/third-party-cyber-security-strengthening-weak-link/; Steve Earley, "6 Best Practices that Reduce Third-Party Cybersecurity Risk," *Security Magazine*, October 5, 2017, https://www.securitymagazine.com/articles/88378-best-practices-that-reduce-third-party-cybersecurity-risk.

[134] "Assessments: Cyber Resilience Review (CRR)," US-CERT, https://www.us-cert.gov/ccubedvp/assessments; "Cybersecurity Assessment Tool," FFIEC, June 2015, https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_june_2015_pdf2.pdf, page 50.

[135] The European Banking Authority has drafted guidelines for banks on ICT outsourcing: "Consultation Paper: EBA Draft Guidelines on Outsourcing arrangements," European Banking Authority, June 22, 2018, https://eba.europa.eu/documents/10180/2260326/Consultation+Paper+on+draft+Guidelines+on+outsourcing+arrangements+%28EBA-CP-2018-11%29.pdf. See also: Aaron Wooten, "Third-Party Cyber Security: Strengthening the Weak Link," CSO Australia, July 2, 2018, https://www.cso.com.au/article/643238/third-party-cyber-security-strengthening-weak-link/; Matthew J. Butkovic and Samuel A. Merrell, "Cybersecurity SLAs: Managing Requirements at Arm's Length," RSA Conference 2013, https://www.rsaconference.com/writable/presentations/file_upload/grc-f42.pdf; "Best Practices in Cyber Supply Chain Risk Management," National Institute of Standards and Technology, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf; Jeffrey Korte, FS-ISAC.

[136] Matthew J. Butkovic and Samuel A. Merrell, "Cybersecurity SLAs: Managing Requirements at Arm's Length," RSA Conference 2013, https://www.rsaconference.com/writable/presentations/file_upload/grc-f42.pdf.

[137] Ten Cybersecurity Tips for Small Businesses," Federal Communications Commission, May 16, 2011, https://www.fcc.gov/document/ten-cybersecurity-tips-small-businesses.

[138] https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

[139] Eric Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Internet Engineering Task Force, March 20, 2018, https://tools.ietf.org/html/draft-ietf-tls-tls13-28#section-11.

[140] "Best Practices in Cyber Supply Chain Risk Management," National Institute of Standards and Technology, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

[141] Steve Earley, "6 Best Practices that Reduce Third-Party Cybersecurity Risk," *Security Magazine*, October 5, 2017, https://www.securitymagazine.com/articles/88378-best-practices-that-reduce-third-party-cybersecurity-risk.

[142] "Fundamental Elements of Cybersecurity for the Financial Sector," G7, October 11, 2016, https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf.

[143] "Information Sharing Resources," Investment Company Institute, https://www.ici.org/info_security/sharing; "Cybersecurity Resource Guide for Financial Institutions," FFIEC, October 2018, https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf; Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/; "Cyber Information Sharing and Collaboration Program (CISCP)," U.S. Department of Homeland Security, September 25, 2018, https://www.dhs.gov/ciscp.

[144] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, and Clem Skorupka, "Guide to Cyber Threat Information Sharing," National Institute of Standards and Technology, October 2016, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf.

[145] "Fundamental Elements of Cybersecurity for the Financial Sector," G7, October 11, 2016, https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf.

[146] "Automated Indicator Sharing (AIS)," US-CERT, https://www.us-cert.gov/ais.

[147] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012,

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf; "Cyberplanner," Federal Communications Commission, https://www.fcc.gov/cyberplanner; Jason Creasey, "Cyber Security Incident Response Guide," CREST, 2013, https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf; "Good cyber security – the foundations," Financial Conduct Authority, 2017, https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf. The UK's FCA offers specific advice on responding to ransomware attacks: " How to react to a ransomware attack," UK Financial Conduct Authority, 2018, https://www.fca.org.uk/publication/documents/ransomware-infographic.pdf.

148 "IT-Grundschutz An Overview: Decision Guide for Managers," Bundesamt für Sicherheit in der Informationstechnik, April 2013, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/IT-Grundschutz_Guide_for_Managers.pdf?__blob=publicationFile&v=1; Stephen Irwin, "Creating a Threat Profile for Your Organization," SANS Institute Reading Room, September 8, 2014, https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492.

149 "Consultation Paper on draft Guidelines on major incidents reporting under the Payment Services Directive 2," Europan Banking Authority, December 7, 2016, https://eba.europa.eu/documents/10180/1688810/Consultation+Paper+on+the+Guidelines+on+Major+Incidents+Reporting+under+PSD2+%28EBA-CP-2016-23%29.pdf.

150 Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Regulators will provide information on expected security practices and reporting requirements, such as in the UK: "Good cyber security – the foundations," UK Financial Conduct Authority, 2017, https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf.

151 Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

152 Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

153 "Cyber Incident Response Plan and Resources," session at 2018 FINRA Cybersecurity Conference, February 22, 2018, http://www.finra.org/sites/default/files/2018_CC_Cyber_Incident_Response.pdf.

154 "Insider Threat Best Practices Guide, 2nd Edition," Securities Industry and Financial Markets Association, February 2018, https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf; Randy Trzeciak, "5 Best Practices to Prevent Insider Threat," Carnegie Mellon University Software Engineering Institute Blog, November 6, 2017, https://insights.sei.cmu.edu/sei_blog/2017/11/5-best-practices-to-prevent-insider-threat.html.

155 See, for example, features offered by Microsoft to track emails ("Manage journaling," Microsoft, December 21, 2018, https://docs.microsoft.com/en-us/exchange/security-and-compliance/journaling/manage-journaling) and third party services such as TheOneSpy (https://www.theonespy.com/) and EmailAnalytics (https://emailanalytics.com/) for Gmail accounts.

156 "Can employers legally monitor employees' emails at work?" GDPR Report, November 17, 2017, https://gdpr.report/news/2017/11/17/5383/.

157 Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

158 Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

[159] Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html; "Cyberplanner," Federal Communications Commission, https://www.fcc.gov/cyberplanner.

[160] "FFIEC Information Technology Examination Handbook: Information Security," Federal Financial Institutions Examination Council, September 2016, https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiid-incident-response.aspx.

[161] Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

[162] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, page 25.

[163] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, page 26; "How to detect a hacker attack," Kaspersky Lab Encyclopedia, https://encyclopedia.kaspersky.com/knowledge/how-to-detect-a-hacker-attack/.

[164] Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

[165] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf; Jason Creasey, "Cyber Security Incident Response Guide," CREST, 2013, https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

[166] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[167] Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

[168] Jason Creasey, "Cyber Security Incident Response Guide," CREST, 2013, https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

[169] Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

[170] Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

[171] Gary Hayslip, "Incident management for SMBs," CSO Online, March 28, 2018, https://www.csoonline.com/article/3267107/data-protection/incident-management-for-smbs.html.

[172] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[173] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, page 43.

[174] Glenn Kennedy, "Security Incident Handling in Small Organizations," SANS Institute, 2008, https://www.sans.org/reading-room/whitepapers/incident/security-incident-handling-small-organizations-32979; "Cyberplanner," Federal Communications Commission, https://www.fcc.gov/cyberplanner; "Computer Security Incident Response Plan," Carnegie Mellon Information Security Office, February 23, 2015, https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan1.0.pdf.

175 Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide: Recommendations from the National Institute of Standards and Technology," National Institute of Standards and Technology, August 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[176] "FFIEC Information Technology Examination Handbook: Information Security," Federal Financial Institutions Examination Council, September 2016, https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiid-incident-response.aspx.

[177] Jason Creasey, "Cyber Security Incident Response Guide," CREST, 2013, https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf, page 45.

[178] "Cyber Security: Small Business Guide," UK National Cyber Security Centre, October 11, 2017, https://www.ncsc.gov.uk/collection/small-business-guide?curPage=/collection/small-business-guide/cyber-security-small-business-guide-infographic.