EXECUTIVE SUMMARY AND PROJECT METHODOLOGY

Capacity-Building Tool Box for Cybersecurity and Financial Organizations

Tim Maurer, Kathryn Taylor, and Taylor Grossman
About the Authors

**Tim Maurer** is director of the Cyber Policy Initiative and a senior fellow in Carnegie’s Technology and International Affairs program. He works on the geopolitical implications of the Internet and cybersecurity, with a focus on the global financial system, influence operations, and other areas of importance as actors exploit the gray space between war and peace. In 2018, Cambridge University Press published his book *Cyber Mercenaries: The State, Hackers, and Power*, a comprehensive analysis examining proxy relationships between states and hackers.

**Kathryn Taylor** is a nonresident expert with the Cyber Policy Initiative at the Carnegie Endowment for International Peace where she helped develop the cyber resilience capacity-building tool box. She is a graduate of Emory University with degrees in computer science and international studies. Currently, she is pursuing her J.D. at New York University School of Law.

**Taylor Grossman** is a research analyst with the Cyber Policy Initiative at the Carnegie Endowment for International Peace, where she works on capacity-building and financial inclusion in the financial sector. She holds an MPhil in International Relations from the University of Oxford and a BA in Political Science from Stanford University.

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, Alejandro Fernández-Cernuda, Terry Wilson, and Kayle Giroud, Global Cyber Alliance; Shafique Ibrahim, Al Fardan Group; Silvia Baur-Yazbeck and David Medine, Consultative Group to Assist the Poor; David van Duren and Chris Painter, Global Forum on Cyber Expertise; Sultan Meghji, Carnegie Endowment for International Peace; Sean Doyle and Nayia Barmpaliou, World Economic Forum; John Carlson, AWS; Nina Paine, Standard Chartered; Peter Meehan and Scott Jackson, iQ4; Kiersten Todt, Cyber Readiness Institute; Paul Makin, Trouver; Keith Bowie, Columbia Business School; Joel Williquette and Steven Estep, Independent Community Bankers of America; Hardeep Mehrotara, Coast Capital Savings; the experts at the FS-ISAC; the experts at the UK Financial Conduct Authority; the experts at the IMF; the experts at the SWIFT Institute; and the experts at the World Bank. Several experts from other institutions who shared feedback preferred to remain anonymous.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPMI-IOSCO</td>
<td>Committee on Payments and Market Infrastructures – International Organization of Securities Commissions</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FCC</td>
<td>U.S. Federal Communications Commission</td>
</tr>
<tr>
<td>FFIEC</td>
<td>U.S. Federal Financial Institutions Examination Council</td>
</tr>
<tr>
<td>FSB</td>
<td>Financial Stability Board</td>
</tr>
<tr>
<td>FS-ISAC</td>
<td>Financial Services – Information Sharing and Analysis Center</td>
</tr>
<tr>
<td>FTC</td>
<td>U.S. Federal Trade Commission</td>
</tr>
<tr>
<td>GDPR</td>
<td>EU General Data Protection Regulation</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>NCSC</td>
<td>UK National Cyber Security Centre</td>
</tr>
<tr>
<td>NIS</td>
<td>Directive EU Directive on the security of network and information systems</td>
</tr>
<tr>
<td>NIST</td>
<td>U.S. National Institute of Standards and Technology</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for Worldwide Interbank Financial Telecommunication</td>
</tr>
</tbody>
</table>
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.” 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 United States and, on the industry side, from SWIFT’s Customer Security Program to FS-ISAC and Sheltered Harbor.

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. 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. 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. Moreover, incidents dating back to 2016 suggest that some threat actors specifically target financial organizations in the Global South and low-income countries.

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, ransomware attacks, and workforce development; 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 particular, 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.

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

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
- Ransomware Guide
- Workforce Development Guide
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. Earlier in 2020, we initiated an update to these guides by soliciting another round of feedback from high-level stakeholders across the financial and cybersecurity sectors. From these discussions, we made a number of changes to the existing guides and also determined a need for two new one-page guides to address growing concerns around ransomware and workforce development, respectively.

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. 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

1 Board-Level Guide: Cybersecurity Leadership
2 CEO-Level Guide: Cybersecurity Leadership
3 CISO-Level Guide: Protecting the Organization
4 CISO-Level Guide: Protecting the Customers
5 CISO-Level Guide: Protecting Connections to Third Parties
6 Incident Response Guide
7 Ransomeware Guide
8 Workforce Development Guide
**What’s in the Package:** Our series of eight 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. Two newly added guides highlight challenges posed by ransomware and long-term workforce development. 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 throughout 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 ten languages: English, French, Spanish, Portuguese, Arabic, Chinese, Russian, Japanese, Mandarin, and Hindi. 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; Taylor Grossman, taylor.grossman@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.
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 on (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.
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.

**ONE-PAGER #7: Ransomware: Prevention and Protection**

Ransomware is a growing threat since malicious actors have found way to monetize malware paralyzing computer systems and demanding a ransom be paid for their release. Unlike other malware, which often has to stay hidden for long periods of time to operate effectively, ransomware is engineered to execute quickly through spear-phishing, compromised websites, and corrupted downloads. Financial institutions are particularly vulnerable to the impact of ransomware because these attacks can threaten the ability to move funds quickly and efficiently and because these organizations are considered lucrative targets. However, bad actors sometimes break their promises: even after a ransom is paid, some attackers do not remove the malware or release confidential data. To guide best practices in prevention and protection, this guide outlines recommendations in the following areas:

- **Gauging Ransomware Readiness** – Providing a framework for developing a ransomware plan.
• **Data Backups** – Creating a system of reliable data backup and recovery procedures.

• **Regulatory Environment** – Understanding changing local and global regulations that deal with ransomware and ransom payments for financial institutions.

**ONE-PAGER #8: Workforce Development**

In order to develop long-term cybersecurity capacity and resilience, an organization needs to invest in its workforce by recruiting and retaining top talent. A gap already exists between supply and demand of cybersecurity skill across sectors. Organizations need to invest in both the short- and long-term health of their cybersecurity workforce by approaching talent recruitment and employee cultivation more creatively and more holistically. This guide offers several external and internal approaches to workforce development.

• **Fundamental Approaches** – Providing five core strategies for developing a robust workforce.

• **Identifying Needs** – Helping organizations understand and evaluate their workforce needs across departments.

• **Improving External Recruitment** – Identifying tools for expanding and streamlining current recruitment models.

• **Advancing Internal Training and Development** – Cultivating existing talent through career mapping and continuing studies.

**Supplementary Report Overview**

The supplementary comprehensive report consists of eight 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.
Notes


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


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.
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 organization’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.
- Regularly review third-party risks.
- 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 gaps in information sharing.

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.
CEOs 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,
  - Evaluating and earmarking funds to invest in security and address existing gaps,
  - 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.

☐ Integrate an assessment of an organization’s cybersecurity when considering mergers and acquisitions.

☐ Institute an annual review of the organization’s cybersecurity policies.

☐ Encourage technical personnel to engage in voluntary information sharing about cybersecurity threats and incidents.
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 technologies that might be used in the event of a work from home deployment.
  - 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 month.

☐ Create a cybersecurity policy for your organization, including a “work from home” protocol.

☐ 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.

☐ Develop a protection plan against insider threats, including enterprise-risk assessment and access control management.

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.
  - Ensure security tools can operate effectively in a “work from home” environment.

☐ 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, including at-home IT infrastructure,
- 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.
<table>
<thead>
<tr>
<th>CONTROLLING PERMISSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Ensure that all personnel have uniquely identifiable accounts that are authenticated</td>
</tr>
<tr>
<td>each time they access your systems.</td>
</tr>
<tr>
<td>□ Only give administrative privileges to trusted IT staff and key personnel and</td>
</tr>
<tr>
<td>revoke administrator privileges on workstations for standard users.</td>
</tr>
<tr>
<td>□ Only give employees access to the specific data systems that they need for their jobs</td>
</tr>
<tr>
<td>and ensure they cannot install any software without permission.</td>
</tr>
<tr>
<td>□ Create user accounts for each employee on your organization’s computers.</td>
</tr>
<tr>
<td>□ Define clear access options for staff and administrators working remotely.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECURING YOUR WI-FI</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Make sure your workplace Wi-Fi is secure and encrypted with WPA2. Routers often</td>
</tr>
<tr>
<td>come with encryption turned off, so make sure to turn it on. Password protect access</td>
</tr>
<tr>
<td>to the router, and make sure that the password is updated from the pre-set default.</td>
</tr>
<tr>
<td>Turn off any “remote management” features.</td>
</tr>
<tr>
<td>□ Limit access to your Wi-Fi network by only allowing devices with certain media</td>
</tr>
<tr>
<td>access control addresses. If customers need Wi-Fi, set up a separate public network.</td>
</tr>
<tr>
<td>□ Enable Dynamic Host Configuration Protocol (DHCP) logging on your networking</td>
</tr>
<tr>
<td>devices to allow for easy tracking of all devices that have been on your network.</td>
</tr>
<tr>
<td>□ Log out as administrator after you have set up the router.</td>
</tr>
<tr>
<td>□ Keep your router’s software up to date. Register your router with the manufacturer</td>
</tr>
<tr>
<td>and sign up to get updates.</td>
</tr>
</tbody>
</table>

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

ADMISTERING 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.
- 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.
- Encrypt customer data in transit and at rest.
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.

CarnegieEndowment.org
CHOOSING VENDORS WITH CYBERSECURITY IN MIND

Each time you are evaluating a potential vendor, check off the following questions:

☐ What experience do they have serving clients similar to your organization?

☐ Have they documented their compliance with known cybersecurity standards (such as the NIST Framework or ISO 27001, or can they provide a SOC2 report)?

☐ Which of your data and/or assets will they need to access to perform their services, and are they requesting any apparently unnecessary access?

☐ How do they plan to protect your organization’s assets and data that are in their possession?

☐ How do they manage their own third-party cyber risk, and can they provide information about their supply chain security?

☐ What is their plan for disaster recovery and business continuity in case of an incident impacting your organization?

☐ How will they keep your organization updated in terms of communicating trends, threats, and changes within their organization?

IDENTIFYING RISK THROUGH THIRD PARTIES

Perform a third party cyber risk assessment including the following steps:

☐ Create and continuously update a list of all vendor relationships and the assets and data that are exposed in each.

☐ Conduct a review of the data that each vendor or third party has access to, ensuring that each level of access adheres to the principle of “least privilege.”

☐ Rank your vendor and third party relationships (low, medium, high) based on the impact that a breach of their systems would have on your organization.

☐ Starting with the highest risk vendors, evaluate each provider’s cybersecurity capabilities and compliance with relevant standards.

☐ Develop a plan for regular security evaluation, keeping in mind that you may occasionally want to conduct on-site assessments of vendors with the highest risk and/or greatest access to customer data.

MANAGING THIRD PARTY SECURITY

☐ Perform thorough due-diligence. Establish cybersecurity expectations in all requests for proposals, contracts, business continuity, incident response, and service level agreements with vendors. Agree on responsibilities and liabilities in case of a cyber incident.

☐ Inquire about the cybersecurity practices of financial organizations and other entities with which you transact or share data, keeping in mind that your vendors and third parties should also be following any cybersecurity requirements that your organization must meet.
Use established and agreed upon measures to monitor your vendors’ compliance with cybersecurity standards.

Check with your vendors that handle sensitive data to see if they offer two-factor authentication, encryption, or other security measures for any accounts you have with them.

Ensure that all third party software and hardware you install have a security handshake so that booting processes are secured via authentication codes and will not execute if codes are not recognized.

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

Annually evaluate vendor contracts and ensure that they continue to meet your strategic direction and regulatory data security requirements. Upon contract termination, include stipulations about getting your assets or data back and verifying that the assets or data are completely erased on the vendor’s side, and disable any access to your systems or servers.

SHARING INFORMATION

Ensure that you have clear communication channels and points of contact to communicate about security issues with your organization’s vendors and counterparts.

Check that you have procedures in place to ensure timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector).

Track relevant updates about what other organizations are experiencing with their third parties in terms of threats, vulnerabilities, incidents, and responses by becoming part of information-sharing organizations like FS-ISAC and seeking other threat information sources.
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.
As you develop a ransomware prevention and protection plan, periodically assess the following:

- Does your organization have regularly scheduled backups?
- Are any nonessential devices connected to your organization’s network?
- Does your organization understand the regulatory and legal risks involved with paying a ransom?
- Does your organization regularly update its software systems? Are these updates automated?
- Does your organization have a plan to deal with a ransomware attack and data loss?
- Does your system have a cyber insurance policy? If so, how does that plan cover ransomware attacks?

Invest in anti-malware protection systems that adapt to new threat intelligence in real-time.

- Evaluate the security of all devices connected to networks that house sensitive or essential information.
  - Connect all nonessential systems to a separate network.
  - Consider the security of remote work setups. Ensure security tools work off-network to monitor all web traffic.

- Promote employee education around phishing attacks and the necessity of strong password protections.

- Consider implementing multifactor authentication across your organization if feasible.

- Keep all software and systems regularly updated.
  - Change settings to allow for automated updates if possible.

- Develop an incident response and crisis management plan for how to deal with a ransomware attack and the loss of valuable data.
  - Prepare an external communication plan in the event of a ransomware attack.

Invest in secure, regularly updated backup systems that keep your data protected.

- If using USBs or hard drives, physically disconnect these devices from networked computers after backups are finished.

- If using cloud storage, equip servers with high-level encryption and multifactor authentication.

- Create a read-only copy of the general ledger for worst-case disaster recovery.

- Develop systems that perform automated data recovery and remediation.

- Develop scenarios to assess how long it will take to recover critical data and business services.
REGULATORY ENVIRONMENT

☐ Evaluate the relevant regulatory and legal guidance for ransomware in your operating environment.
  ☐ Consider country-specific guidance.
  ☐ Consider financial-sector specific guidance.
  ☐ Consider international legal and regulatory requirements.
  ☐ Develop a plan for periodic evaluation of changing guidance.

☐ Assess risks involved with paying a ransom.
☐ Liaise with local law enforcement.
☐ Build connections for quick information sharing in the event of an attack.
☐ Assess the benefits and drawbacks of cyber insurance policies for ransomware.
FUNDAMENTAL APPROACHES TO CYBERSECURITY WORKFORCE DEVELOPMENT

☐ Expand the supply pipeline.
  • Does your organization have relationships with universities and technical colleges?
  • Do you offer cybersecurity internships and apprenticeships?

☐ Identify and match existing supply with talent openings.
  • Is your human resources department effectively translating required skills into posted job descriptions?

☐ Retrain existing staff to become part of the cyber workforce.
  • Is your organization leveraging existing talent by shifting resources to its cyber workforce?

☐ Reduce the demand on your cyber workforce through technological innovation.
  • Do you have agreements with third-party service providers to create surge capacity?

☐ Improve retention of the current workforce.
  • Is your organization investing in talented team members?
  • Does your organization allow interested individuals to explore careers in cybersecurity?

IDENTIFYING NEEDS

☐ Identify your workload requirements.
  ☐ Evaluate the complexity of your operations and the speed with which actions need to be executed.
  ☐ Consider surge capacity needs and whether advanced technologies can help reduce attack surface.

☐ Identify your workforce requirements.
  ☐ Consider the competency, flexibility, and agility of the cybersecurity workforce in your organization.
  ☐ Identify ideal reporting structures and highlight where multi-functionality is preferable.

☐ Define the required knowledge, skills, abilities, and competency of your cybersecurity workforce based on the business functions they support.

☐ Identify critical gaps in your organization’s existing cybersecurity workforce.
  ☐ Employ existing tools such as the NICE framework to guide internal assessments of roles and responsibilities.
IMPROVING EXTERNAL RECRUITMENT

- Strengthen job postings by writing clear, internally consistent job descriptions.
  - Use existing tools such as the NICE framework to highlight relevant skill sets.
- Gather data on recruitment through the application process.
  - Systematize data collection and share throughout the company to prevent silo formation and support talent sourcing and development.
  - Evaluate recruitment data periodically to identify gaps in outreach.

- Rely on multiple indicators to assess candidate potential.
  - Consider implementing systematized hiring assessments.
  - Evaluate relevant degrees, certifications, and work experiences.
  - Avoid relying on one specific metric when making hiring decisions.

ADVANCING INTERNAL TRAINING AND DEVELOPMENT

- Develop career maps that highlight advancement tracks for your cybersecurity workforce.
- Identify pathways within your organization for retraining and repositioning staff into cybersecurity roles.
  - Consider potential nontraditional entry points into cybersecurity based on interest and ability.
  - Expand upskilling and retraining programs and incentivize transitions within your organization.
- Encourage internal training and independent learning.
  - Open opportunities for continued education and skill certification.
- Track data on workforce retention.
  - Evaluate retention data periodically to identify whether programs are meeting employee needs.
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. Regularly review third-party risks.
- 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 gaps in information sharing.

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.

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 incident response plans 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?
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,
  • Evaluating and earmarking funds to invest in security and address existing gaps,
  • Continuously reevaluating your organization’s cybersecurity maturity, risks, and goals,
  • Considering using third party penetration-testing or red-teaming, and
  • 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, including adequate budgeting, 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.
• Integrate an assessment of an organization’s cybersecurity when considering mergers and acquisitions.
• Annually review your organization’s cybersecurity policies.
• Encourage voluntary information sharing about cybersecurity threats and incidents within your organization and with trusted counterparts.
• Foster innovation that incorporates security concerns and planning from the outset.
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).
   - 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.

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 month.
   - Develop a protection plan against insider threats that includes an enterprise-wide risk assessment and strict management of access controls.

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. This should include a clear and well-known “work from home” protocol.

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 anti-virus software and anti-spyware on all computers and laptops. To protect a distributed workforce, ensure that security tools can operate effectively in a “work from home” environment.
- 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, including at-home IT infrastructure,
  - 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.
- Define clear access options for staff and administrators working remotely.

**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.
- 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).
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.
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.
How to Choose Vendors With Cybersecurity in Mind

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

1. What experience do they have? Find out about the vendor’s history serving clients. Have they served clients similar to your organization before?

2. Have they documented their compliance with known cybersecurity standards such as the NIST Framework or ISO 27001, or can they provide a SOC2 report?

3. Which of your data and/or assets will they need to access to perform their services? Are they requesting any apparently unnecessary access?

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

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

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

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

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.

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.
Gauging Your Organization’s Ransomware Readiness

Consider the following questions when developing a ransomware prevention and protection plan.

1. Does your organization have regularly scheduled backups?
   - Are these backups disconnected from your network, either via cloud storage systems or air-gapped USBs/hard drives?

2. Are any nonessential devices connected to your organization’s network?
   - Can they be moved to other networks that do not house sensitive data?

3. Does your organization understand the regulatory and legal risks involved with paying a ransom?
   - Legal guidance on this varies from country to country and is frequently updated.

4. Does your organization regularly update its software and systems? Are updates automated?

5. Does your organization have a plan for how to deal with a ransomware attack and the loss of valuable data?

6. Does your organization have a cyber insurance policy? If so, how does that plan cover ransomware attacks?
   - Some plans explicitly prohibit ransom payments, while others will cover such a payment as part of the policy.

RANSOMWARE: PREVENTION AND PROTECTION

REAL-TIME PROTECTION

Ransomware is a growing threat since malicious actors have found ways to monetize malware paralyzing computer systems and demanding a ransom be paid for their release. Unlike other malware, which often has to stay hidden for long periods of time to operate effectively, ransomware is engineered to execute quickly through spear-phishing, compromised websites, and corrupted downloads. Financial institutions are particularly vulnerable to the impact of ransomware because these attacks can threaten the ability to move funds quickly and efficiently and because they are considered lucrative targets. However, bad actors sometimes break their promises: even after a ransom is paid, some attackers do not remove the malware or release confidential data.

- Invest in anti-malware protection systems that adapt to new threat intelligence in real-time.
- Evaluate the security of all devices connected to networks that house sensitive or essential information. Connect all nonessential systems to a separate network.
  - Be particularly careful when bringing IoT or “smart devices” into your workspaces, since these systems often have weaker or nonexistent security systems and can be targeted as access points to essential systems.
- Consider the security of remote work setups. Ensure security tools work off-network to monitor all web traffic.
- Promote employee education around phishing attacks and the necessity of strong password protections.
- Consider implementing multifactor authentication across your organization if feasible.
- Keep all systems and software regularly updated. Change settings to allow for automated updates if possible.
- Develop an incident response and crisis management plan for how to deal with a ransomware attack and the loss of valuable data.
- Prepare an external communication plan in the event of a ransomware attack.

DATA BACKUPS

- Invest in secure, regularly updated backup systems that keep your data protected.
  - If using USBs or hard drives, physically disconnect these devices from networked computers after backups are finished.
  - If using cloud storage, equip server with high-level encryption and multifactor authentication.
- Create a read-only copy of the general ledger for worst case disaster recovery.
- Develop systems that perform automated data recovery and remediation.
- Develop scenarios to assess how long it will take to recover critical data and business services.

REGULATORY ENVIRONMENT

- Evaluate the relevant regulatory and legal guidance for ransomware in your operating environment.
  - Consider country-specific guidance. Develop a plan for periodic evaluation of changing guidance.
  - Consider financial-sector specific guidance.
  - Consider international legal and regulatory requirements.
- Assess risks involved with paying a ransom. In some cases, paying a ransom could violate existing sanctions regimes in place against hostile actors.
- Liaison with local law enforcement. Build connections for quick information sharing in the event of an attack.
- Assess the benefits and drawbacks of cyber insurance policies for ransomware.
WORKFORCE DEVELOPMENT

IDENTIFYING NEEDS

• Identify your workload requirements.
  • Evaluate the complexity of your operations and the speed with which actions need to be executed.
  • Consider surge capacity needs and whether advanced technologies can help reduce the attack surface.

• Identify your workforce requirements.
  • Consider the competency, flexibility, and agility of the cybersecurity workforce in your organization.
  • Identify ideal reporting structures and highlight where multi-functionality is preferable.

• Define the required knowledge, skills, abilities, and competency of your workforce based on the roles they occupy and the business functions they support.

• Identify critical gaps in your organization’s existing cybersecurity workforce.
  • Employ existing tools such as the NICE framework to guide internal assessments of roles and responsibilities.

ADVANCING INTERNAL TRAINING AND DEVELOPMENT

• Develop career maps that highlight advancement tracks for your cybersecurity workforce.

• Identify pathways within your organization for retraining and repositioning talented staff into cybersecurity roles.
  • Consider potential nontraditional entry points into cybersecurity based on interest and ability.
  • Expand upskilling and retraining programs and incentivize transitions within your organization.

• Encourage internal training and independent learning.
  • Open opportunities for continued education and skill certification.

• Track data on workforce retention.
  • Evaluate retention data periodically to identify whether training and development programming is meeting employee needs.

IMPROVING EXTERNAL RECRUITMENT

• Strengthen job postings by writing clear, internally consistent job descriptions.
  • Use existing tools such as the NICE framework to highlight relevant skill sets.

• Gather data on recruitment through the application process, capturing types of applicants and previous work experiences.
  • Systematize data collection and share throughout company to prevent silo formation and support talent sourcing and development.
  • Evaluate recruitment data periodically to identify gaps in outreach.

• Rely on multiple indicators to assess candidate potential.
  • Consider implementing systematized hiring assessments.
  • Evaluate relevant degrees, certifications, and work experiences.
  • Avoid relying on one specific metric (e.g., a masters-level degree in engineering) when making hiring decisions.

Fundamental Approaches

Consider the following strategic approaches when developing a cybersecurity workforce.

1. Expand the supply pipeline producing new talent.
   • Do you have relationships with universities and technical colleges?
   • Do you offer cybersecurity internships or apprenticeships?

2. Identity and match existing supply with talent openings.
   • Is your human resources department effectively translating required skills into posted job descriptions?

3. Retrain existing staff to become part of the cyber workforce.
   • Is your organization leveraging existing talent by shifting resources to its cyber workforce?

4. Reduce the demands on your cyber workforce through technological innovation.
   • Do you have agreements with third-party service providers to create surge capacity during critical periods?

5. Improve retention of the current workforce.
   • Is your organization investing in talented team members?
   • Does your organization allow interested individuals to explore careers in cybersecurity?