CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

DECEMBER 2020

EXECUTIVE SUMMARY AND PROJECT METHODOLOGY

Capacity-Building Tool Box for Cybersecurity and Financial Organizations

Tim Maurer, Kathryn Taylor, and Taylor Grossman


EXECUTIVE SUMMARY AND PROJECT METHODOLOGY

Capacity-Building Tool Box for Cybersecurity and Financial Organizations

Tim Maurer, Kathryn Taylor, and Taylor Grossman

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

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

CONTENTS

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.

Official Partners

Glossary

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

Executive Summary

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

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

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

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

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

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

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

Multiple Feedback Loops: Upon reviewing existing material, we shared drafts with experts from a variety of national and international institutions to gauge the relative utility and practicability of the various strategies and measures. Engaging with experts from several central banks and commercial banks as well as other institutions including the IMF, FS-ISAC, and SWIFT enabled us to synthesize the patchwork of existing guidance into a package of targeted, high-yield recommendations for less cyber-mature and smaller financial organizations. 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.[10] Yet, as this research progressed, it became clear that effective cybersecurity guidance must inform behavior not only at the technical level but at many other decision points, from executive strategy to employee awareness to third party interactions. This led us to develop mutually reinforcing sets of best practices for CEOs and chief information security officers (CISOs) that, altogether, cover governance, IT measures, employee training and behavior, customer data security, vendor management, and organization-wide incident response.

FIGURE 1

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

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 Document*s: 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.

ONE-PAGER #2: CEO-Level Guide

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

- *Governance* – Positioning executives as the leaders of their organizations' cybersecurity by advising them to appoint and articulate roles and responsibilities for cybersecurity staff and to direct efforts to establish organization-wide cybersecurity policies and practices applicable to every member of staff.
- *Risk Assessment and Management* – Directing executives to call for and oversee cyber risk assessment, to digest the results and operationalize them in organizational decision-making, and to ensure ongoing monitoring of cyber risk.
- *Organizational Culture* – Advising executives to include cybersecurity considerations in overall organizational thinking and decision-making and to foster an organization-wide culture of cybersecurity by instituting regular trainings and reviews and making cybersecurity a normal part of communication at all levels.

Guidance for CISOs and Other Personnel: Technical Improvements

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

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

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

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

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

- *Preventing Malware Damage* – Describing essential cybersecurity practices that CISOs should engage in to secure their organizations' systems such as using firewalls, antivirus software, pen-testing, red-teaming, and physical security measures.
- *Training Employees* – Advising CISOs to make regular, comprehensive staff cybersecurity education a key priority.
- *Protecting Data* – Advising CISOs to keep updated and segmented backups and to take other data protection measures.
- *Securing Devices* – Advising CISOs on how to configure, secure, and handle the life cycle of their organizations' computers, laptops, mobile phones, and other devices.
- *Using Passwords* – Detailing how CISOs should set up password use across their organization and advise employees on how to use secure authentication.
- *Controlling Permissions* – Advising CISOs on how to manage administrative and general employee privileges on their organizations' systems and data.
- *Securing Wi-Fi* – Advising CISOs on how to securely configure their organizations' wireless Internet networks.
- *Avoiding Phishing Attacks* – Identifying the most common indicators of phishing, advising CISOs on preventive steps to take, and advising all employees to stay alert.

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

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

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

- *Administering Accounts* – Advising CISOs on how to create and manage customer accounts so that a high level of security is offered by default.
- *Protecting Data* – Advising CISOs to securely handle and store customer information with strong data policies and measures such as encryption.
- *Securing Public Web Applications* – Providing steps for CISOs to take to secure all public-facing channels with which customers may interact and provide data.
- *Training Employees* – Advising CISOs to train employees to handle customer data carefully and responsibly.
- *Notifying Customers* – Describing how CISOs should handle customer notification as part of incident response.

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

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

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

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

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

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

ONE-PAGER #6: Incident Response Guide

An organization's cybersecurity is tested when incidents actually occur and their preparation must turn into action. Studies show that many firms do not invest sufficiently in response and recovery. Organizations should be prepared that an incident will occur eventually and need to have a plan for response and recovery. Unfortunately, the question is not one of "if" but of "when" such an incident will occur. Having holistic, well-documented incident response plans in place is therefore so crucial

to cybersecurity in practice that it merits its own section in this report. It is helpful to understand incident response through the pillars of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover (see Appendix). These pillars describe the lifecycle of incident response and have informed the organization of best practices in this section, which focus on:

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

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.
- *Real-Time Protection* – Investing in robust anti-malware protection and crafting emergency response plans.

- *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

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

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

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

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

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

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

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

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

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

10 It is important here to highlight specifically that, while there is growing consensus on the security benefits smaller organizations can gain from migrating to the Cloud, policies remain evolving. We encourage organizations to explore migrating to the Cloud while tracking near- and mid-term policy developments. Our section on Protecting Connections to Third Parties offers more guidance on how to evaluate potential third-party technology providers.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org