TECHNICAL

NOTES & MANUALS

Strengthening Cybersecurity: Lessons from the Cybersecurity Survey

Rangachary Ravikumar

TNM/2025/06

TECHNICAL NOTES AND MANUALS

Strengthening Cybersecurity: Lessons from the Cybersecurity Survey

Rangachary Ravikumar

Authorized for distribution by Tobias Adrian

- This technical note draws lessons from cybersecurity surveys conducted by the IMF's Monetary and Capital Markets Department to provide advice to central banks, supervisory authorities, and policymakers seeking to strengthen the cybersecurity of their financial sectors. The technical note covers various measures adopted by central banks and supervisory authorities, lessons learned from the survey results, and further efforts to strengthen cybersecurity, besides providing references to work by international standard-setting bodies.
- Concerted efforts are needed to (1) develop national and financial sector–focused cybersecurity strategies, (2) build cyber risk regulatory and supervisory capacity, and (3) address resource constraints. Legal and regulatory clarity regarding supervisory powers, adequate attention by top management, and resource augmentation will help supervisory authorities address existing gaps in these areas. Central banks and supervisory authorities also need to develop processes to better understand the threat landscape on a continuous basis. Capacity needs to be augmented in (1) conducting cyber exercises and tests, (2) helping build sectorwide incident response capabilities, and (3) building cyber maps. In addition, special attention is needed toward establishing and nurturing robust institutional arrangements, in terms of enabling legal provisions to criminalize cyberattacks and establishing Computer Emergency Response Teams and Financial Sector Computer Emergency Response Teams.

The author thanks Tamas Gaidosch, Emran Islam, and Tanai Khiaonarong for their useful inputs and comments; Dirk Jan Grolleman, Marina Moretti, and Jay Surti for providing intellectual direction and guidance; Rick Zheng for preparing the figures; and Urgamal Azat for editorial support.

© 2025 International Monetary Fund
Cover Design: IMF Creative Solutions

Cataloging-in-Publication Data
IMF Library

Names: Ravikumar, Rangachary, author. | International Monetary Fund, publisher.
Title: Strengthening cybersecurity : lessons from the cybersecurity survey / Rangachary Ravikumar.
Other titles: Lessons from the cybersecurity survey. | Technical notes and manuals. | International Monetary Fund. Monetary and Capital Markets Department (Series).
Description: Washington, DC : International Monetary Fund, 2025. | Mar. 2025. | Includes bibliographical references.
Identifiers: ISBN:
9798400296864 (paper)
9798400296147 (ePub)
9798400296109 (web PDF)
Subjects: LCSH: Computer security. | Computer networks—Security measures. | Database security.
Classification: LCC QA76.9.A25 2025

DISCLAIMER:
This Technical Guidance Note should not be reported as representing the views of the IMF. The views expressed in this paper are those of the authors and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

Recommended citation:
Ravikumar, Rangachary. 2025. "Strengthening Cybersecurity: Lessons from the Cybersecurity Survey." IMF Technical Notes and Manuals 2025/06. International Monetary Fund, Washington, DC.

Please send orders to:
International Monetary Fund, Publication Services
PO Box 92780, Washington, DC 20090, USA
Tel: (202) 623–7430 | Fax: (202) 623–7201
publications@IMF.org
eLibrary.IMF.org
bookstore.IMF.org

Contents

ABBREVIATIONS

AE	advanced economy
BCBS	Basel Committee on Banking Supervision
BCP	Basel Core Principles for Effective Banking Supervision
CERT	Computer Emergency Response Team
CPI	Cybersecurity Preparedness Index
CPMI	Committee on Payments and Market Infrastructures
FCS	fragile and conflict-affected state
FinCERT	Financial Sector Computer Emergency Response Team
FSB	Financial Stability Board
G7	Group of Seven
IAIS	International Association of Insurance Supervisors
ICT	Information and communications technology
IOSCO	International Organization of Securities Commissions
NIST	National Institute of Standards and Technology
SSBs	standard-setting bodies

I. Executive Summary

Cyber risk has become a prominent risk within the financial sector, and the role of supervisory authorities is increasing. Digitalization of the financial sector, increasing financial and operational interconnectedness, and the higher frequency and sophistication of cyberattacks have encouraged standard-setting bodies (SSBs) to increasingly focus on cyber risk. A survey to understand the cyber preparedness of supervisory authorities addresses information gaps and helps better tailor the IMF's capacity-building initiatives to the member countries' needs and priorities.

The survey questionnaire, centered on common focus areas across the SSBs' work, has 7 themes comprising 42 questions. The survey is addressed to central banks and supervisory authorities, mainly in low- and lower-middle-income countries and is geared toward standardization. For the year 2021, there were 53 responses, and for 2023, there were 74 responses. Thirty-two countries responded to both surveys. Where meaningful, the survey responses received from all the respondents have been used to present the results.

There is progress in strengthening governance and articulating strategy, but gaps remain. National and financial sector–focused cybersecurity strategies have gained prominence, and more jurisdictions have developed such strategies, but more than half of the surveyed jurisdictions are yet to develop such strategies. Governance arrangements show progress as does the coordination between central banks and supervisory authorities where they are different. In the face of bad actors collaborating effectively to launch cyberattacks, supervisory authorities need to strengthen their coordination with other regulators and government agencies.

The number of jurisdictions that have developed cyber risk regulatory frameworks and data privacy regulations and have strengthened supervisory architecture is growing, but more work is required. Building regulatory and supervisory capacity to cope with increased cybersecurity risk is an urgent priority. A targeted approach, based on identified gaps, would yield superior results. Resource constraints could be contributing to suboptimal progress in establishing a supervisory framework for such risks. Cyber risk supervision needs to be strengthened by increasing capacity to conduct on-site examinations and to intensify off-site supervision beyond current levels, extending its scope to critical third parties.

Response and recovery capabilities after cyber incidents remain weak, and testing protocols are under development. Threat intelligence gathering within central banks and supervisory authorities continues to be based predominantly on informal arrangements and individual initiatives. Close to a third of all respondents have yet to establish protocols to handle major cyber incidents in their financial sector. The Financial Stability Board's "Effective Practices for Cyber Incident Response and Recovery" provides useful guidance to strengthen response and recovery capabilities.

Information sharing and incident reporting are key elements in managing cyber risk, and although there has been progress between the surveys, significant gaps remain to be addressed. Despite the significant benefits it provides in tackling cyberattacks, information sharing is not prevalent in about three-quarters of responding authorities Cyber incident reporting regimes are not in place in a majority of surveyed respondents, the articulation of the taxonomy and severity of cyber incidents is lacking, and an incident reporting format has not been prescribed by many jurisdictions. The Financial Stability Board's "Final Report on Recommendations to Achieve Greater Convergence in Cyber Incident Reporting" (FSB 2020) sets out actions and steps that authorities can take to promote convergence among cyber incident reporting frameworks and encourage better practices.

Most of the surveyed jurisdictions criminalize cyberattacks, but more than a third do not have a Computer Emergency Response Team. There is a lack of clarity on how to report cybercrime, retain digital evidence, and transfer this evidence to aid the prosecution of cybercriminals.

Cyber risk analysis needs to be strengthened and incorporated further into financial stability analysis in many emerging market economies. Cyber mapping as a tool is still underdeveloped and under development in most jurisdictions. Adequate information on the financial sector's cloud migration is not available to supervisory authorities and central banks, although, by 2023, the monitoring status had improved relative to two years earlier. Analysis in which a severe cyber incident is considered one of the adverse scenarios is becoming prevalent in stress tests estimating the resilience of liquidity and capital. The other type of stress test focuses on the ability of institutions to respond to, and recover from, cyber incidents and is referred to as a cyber resilience stress test.

Building cybersecurity supervisory capacity requires more attention in most jurisdictions. A lack of resources hampers capacity building, particularly among low- and lower-middle-income countries. Many jurisdictions do not have any plans for capacity building. Requiring certifications in cybersecurity from supervisory staff is slowly improving. Such gaps in capacity building demonstrate the desirability of the IMF playing a proactive role.

Based on the survey results, a cybersecurity preparedness index (CPI) has been built to track progress. Overall, the CPI score improved marginally between 2021 and 2023, with material regional variation. An analysis of the distribution of CPI scores indicates that a large share of respondents has progressed to a higher range of scores.

II. Background and Objectives

Cybersecurity threats are a prominent and rapidly growing risk to the stable and efficient functioning of the financial system—central banks and supervisors have a key role in overseeing the adequate and timely management of this risk. The role of these authorities encompasses the safety and soundness of individual financial institutions, financial infrastructures, and financial markets. The growing risk relevance of cybersecurity is a reflection of the growing adoption of digital technology by financial sector entities and the digitalization of financial products and services that is happening in step with an expansion in digital infrastructures. The increasing number and sophistication of cyberattacks targeting the financial sector provide a powerful indication of the criticality of these risks, with the focus being devoted to systemic cyber risk events, that is, the possibility of a single failure in cyberspace adversely impacting financial stability (Forscey and others 2022).

Global and sectoral financial SSBs are increasingly focusing on cybersecurity risk, including the Group of Seven (G7), the Group of Twenty, the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS). They have conducted or commissioned work on cybersecurity risks including stock takes, surveys of regulatory and supervisory practices, emerging best practices, principles, newsletters, and reporting templates (Figure 1).

Figure 1. Standard Setters' and IMF's Work on Cybersecurity

G7 – Fundamental Elements	CPMI-IOSCO – Cyber Resilience	NIST Cybersecurity Framework 2.0	PSMOR – ICT Risk Management	IMF Paper – Cyber Risk and Financial Stability

• Cybersecurity strategy and framework
• Governance
• Risk and control assessment
• Monitoring
• Response
• Recovery
• Information sharing
• Continuous learning
	• Governance
	• Identification
	• Protection
	• Detection
	• Response and recovery
	• Testing
	• Situational awareness
	• Learning and evolving
		• Governance
		• Identify
		• Protect
		• Detect
		• Response
		• Recovery
			• ICT risk management
			  • Identification and assessment
			  • Risk mitigation measures
			  • Monitoring
			• Alignment of business, risk management, and ICT strategies
			• Regular testing and review
			• Threat intelligence
			• ICT readiness for stressed scenarios
				• Financial stability analysis
				  • Cyber mapping
				  • Quantitative analysis
				  • Stress testing
				• Regulatory and supervisory framework
				• Response and recovery
				• Information sharing
				• Deterrence
				• Capacity building

Sources: G7 Fundamental Elements of Cybersecurity; CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures; NIST Cybersecurity Framework 2.0; Revised Principles for Sound Management of Operational Risk; and IMF's Cyber Risk and Financial Stability: It's a Small World After All.

Note: CPMI-IOSCO = Committee on Payments and Market Infrastructures-International Organization of Securities Commissions; G7 = Group of Seven; ICT = information and communications technology; NIST = National Institute of Standards and Technology; PSMOR = Principles for the Sound Management of Operational Risk.

Common themes drawn from this work on cybersecurity provided the basis for designing the surveys. These themes are (1) governance and strategy; (2) cyber regulation and supervision; (3) monitoring, response, and recovery; (4) incident reporting and information sharing; (5) cyber deterrence; (6) financial stability analysis; and (7) continuous learning and capacity development.

Cybersecurity regulations and supervisory practices have evolved, and a common approach to mitigating cybersecurity risk is arising among some advanced and emerging markets, although the broader

global challenge in this area remains significant. For example, in jurisdictions such as Australia, Canada, the European Union, Hong Kong SAR, and Singapore, technology and cybersecurity regulations or prudential standards issued by supervisory authorities clearly articulate their expectations of supervised entities in a proportional and principles-based manner. Several other jurisdictions such as Ghana, India, Nigeria, and the Philippines have also issued similar regulations.[1] However, many emerging market economies have yet to include information and communications technology (ICT) and cyber risk as part of their regulations. Moreover, there are important gaps in cybersecurity regulations and supervisory practices among low- and lower-middle-income countries, reflecting significant human, technical, and financial resource constraints. Digitalization and digital infrastructures are growing globally, even where there is a lack of cybersecurity readiness, and it is important to understand the gaps in cybersecurity preparedness among supervisors and then address them on a priority basis.

The IMF's capacity-building initiatives are focused on low- and lower-middle-income countries. The demand for bilateral capacity-building activities on cybersecurity risk has increased considerably in recent years. Approximately 50 bilateral capacity-building engagements have been delivered during 2021–23. To tailor these activities better to the needs of the IMF's member countries, a mechanism was sought to deepen the understanding of the regulatory and supervisory landscape within low- and lower-middle-income countries.

Cybersecurity surveys typically do not focus on financial sector authorities. Surveys carried out by the big four audit firms, other consultants, and stakeholders focus more on financial sector entities, the role of their boards, their perspectives on the emerging threats landscape, emerging best practices in mitigating cybersecurity risk, and the cost of cyber incidents. Thus, there is a perceived information gap in terms of our understanding of how well supervisory authorities have coped with emerging cybersecurity threats targeting the financial sector.

To close this information gap, the IMF conducted cybersecurity surveys in 2021 and 2023. The first survey had the objective of collecting data on key elements about cybersecurity of the financial sector and to further aid the IMF in developing tools to build capacity globally. The survey was an important stock take that provided the IMF with valuable insight into the global picture of cybersecurity. The second survey was launched in 2023 to update the information collected in 2021 and gauge new developments. For the year 2021, there were 53 responses, and for 2023, there were 74 responses comprising 8 and 14 fragile and conflict-affected states (FCSs), respectively. The responses covered authorities from around the world, including East Asia and the Pacific (9 in 2021 and 11 in 2023—5 of which responded to both surveys), Europe and Central Asia (8 in 2021 and 11 in 2023—3 of which responded to both surveys), Latin America and the Caribbean (12 in both surveys—7 of which responded to both surveys), Middle East and North Africa (5 in both surveys—2 of which responded to both surveys), South Asia (5 in 2021 and 6 in 2023—5 of which responded to both surveys), and sub-Saharan Africa (14 in 2021 and 29 in 2023—10 of which responded to both surveys). The number of low- and lower-middle-income countries responding in 2021 and 2023 stood at 26 and 47, respectively, followed by upper-middle-income countries at 22 and 23, respectively.

A CPI has been prepared using select survey data.[2] The surveys found that supervisory authorities recognize the importance of cybersecurity and have made progress on adjusting their policies accordingly, but gaps remain. The results indicate that many authorities have put in place national and financial sector cybersecurity strategies, issued regulations focused on ICT/cyber risk, mandated testing arrangements, and introduced incident reporting frameworks. The progress is uneven and marked by resource constraints and

[1] For regulations in Ghana, see https://www.bog.gov.gh/wp-content/uploads/2019/09/CYBER-AND-INFORMATION-SECURITY-DIRECTIVE.pdf; for India, see https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0; and for Nigeria, see https://www.cbn.gov.ng/Out/2024/BSD/CBN%20Risk-Based%20Cybersecurity%20Framework%20for%20DMBs%20and%20PSBs_2024.pdf.

[2] The results of the survey and the CPI are also summarized in IMF (2024).

capacity limitations. In some areas, such as information-sharing arrangements, financial stability analysis, and cyber deterrence, significant gaps remain.

This technical note provides an overview of developing economies' cybersecurity preparedness and existing key gaps. Section III discusses the design of the survey used for the stock take. Section IV focuses on the survey results and the resulting recommendations and direction of the next steps that are necessary to strengthen the cybersecurity of the financial sector. Summarizing the overall developments across participating regions, Section V discusses the main observations of the CPI. Section VI concludes.

III. Survey Design and Response Rate

The survey questionnaire was developed based on 7 themes and comprised 42 questions. The themes cover (1) governance and strategy; (2) cyber regulation and supervision; (3) monitoring, response, and recovery; (4) incident reporting and information sharing; (5) cyber deterrence; (6) financial stability analysis; and (7) continuous learning and capacity development.

These themes are the common elements across global and financial sector SSBs and follow the structure of the standards and papers presented in Figure 1. Because they comprehensively cover the key elements of financial regulation and supervision of cybersecurity, this is also a structure that the IMF's Monetary and Capital Markets Department uses for its cybersecurity capacity development programs. For each of these seven themes, the survey contains 4–10 questions. The survey closes with an open question asking for additional comments. Although the questions do not cover every theme in depth, they are designed to give a view of the key elements and main developments of each.

The design of the survey is geared toward standardization. Most of the questions are multiple choice with instructions, and very few provide an option to choose more than one answer. The survey was launched online, with validations to ensure all critical questions are answered and responses aggregated using Excel utilities. Instructions provided to fill out the survey, as part of the questionnaire, are presented in Annex 2.

The survey mainly targeted supervisory authorities in low- and lower-middle-income countries. It was issued to the authorities of 90 countries that were invited to the IMF's Annual Cybersecurity Workshop. For the year 2021, there were 53 responses, and for 2023, there were 74 responses. Thirty-two countries responded to both surveys. An overview of the respondents' geographical distribution is given in Table 1. Africa and Asia are well represented in the survey followed by Latin America and Europe.

Table 1. An Overview of the Respondents' Geographical Distribution[1]

Region	2021	2023
Africa	16 (*30.2*)	27 (*36.5*)
Asia	17 (*32.1*)	26 (*35.1*)
Europe	8 (*15.1*)	8 (*10.8*)
Latin America	12 (*22.6*)	13 (*17.6*)

Source: Survey responses.

[1]Figures in parentheses denote the percent of total respondents.

IV. Survey Results and Observations and Recommendations

The number of responses received for the 2021 and 2023 surveys varies, with a smaller set of countries responding to both surveys. Where meaningful, the survey responses received from all the respondents have been used. The responses have also been grouped on the basis of the membership of a country into the group of FCS and a country's income level.

A. Governance and Strategy

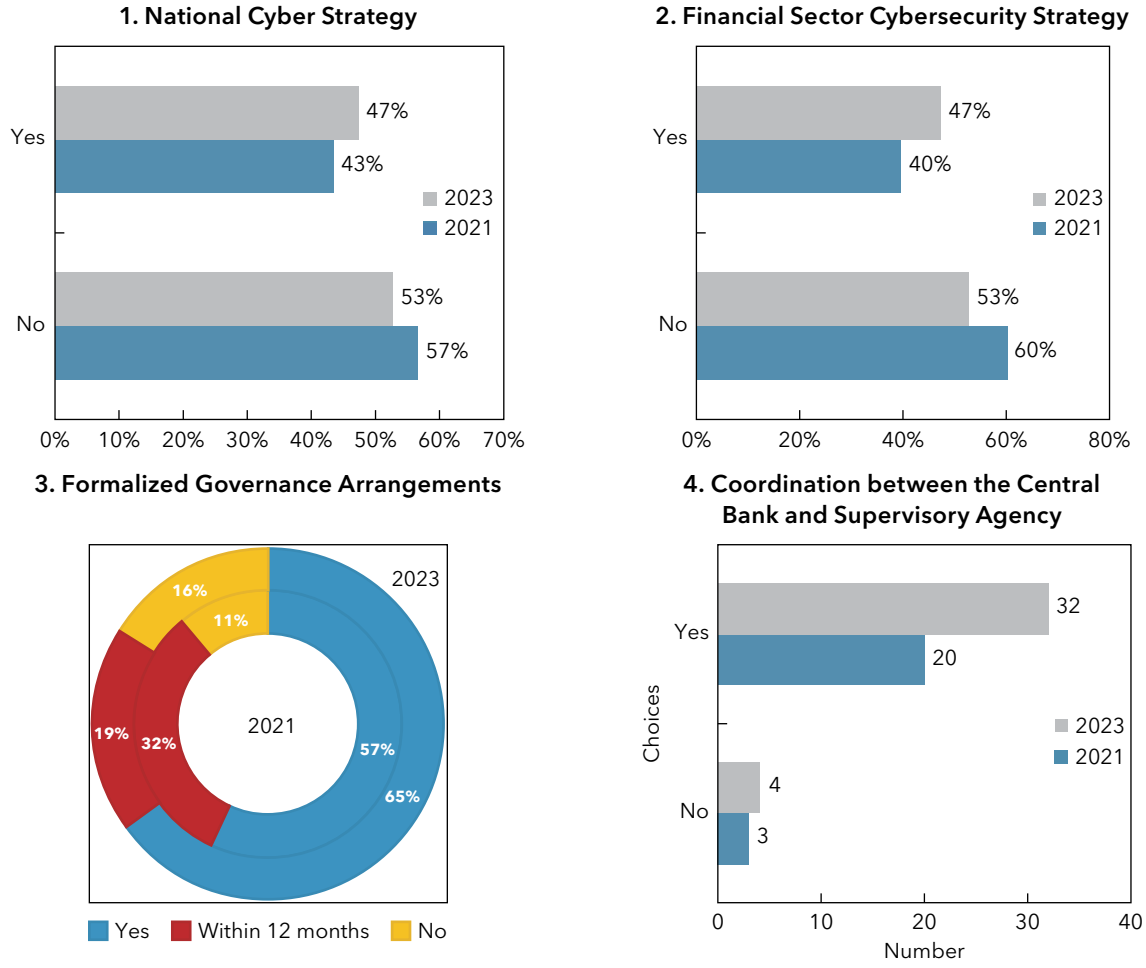
Survey Results

The first theme has six questions focused on governance and strategy. The theme covers the national cybersecurity strategy, the financial sector cybersecurity strategy, the allocation of responsibility to approve the financial cybersecurity strategy, the existence of formalized governance arrangements, the mandates of the central bank and the supervisory agency, and coordination between the central bank and the supervisory agency, where applicable.

Overall, there is little change between 2021 and 2023 in the development of a cybersecurity strategy (Figure 2, panels 1 and 2). More than half of the countries responding to both surveys indicated that they have neither a national cybersecurity strategy nor a financial sector cybersecurity strategy. Respondents that have a national cybersecurity strategy increased by 4 percent to 47 percent, whereas 27 percent of those without a cybersecurity strategy in 2023 planned to have one within a year, an increase from 21 percent in the 2021 survey. A quarter of the respondents neither had a strategy in 2023 nor were planning to develop one, down from one-third in 2021. Reviewing comparable data, that is, responses received for both years from the same respondents, there is no change in the number of jurisdictions having a national cybersecurity strategy, though the number of countries developing one shows a marginal increase across the two surveys.

Arrangements have improved with more than half of the respondents having some form of governance in place (Figure 2, panels 3 and 4). The expectation is that governments in consultation and coordination with supervisory authorities contribute to developing better governance over cybersecurity matters by enabling institutional arrangements. A comparison across countries responding to both surveys indicates that there is an improvement—the share of countries with governance arrangements within the central bank or supervisory authorities increased from 56 percent to 69 percent. Considering all responses, jurisdictions with governance arrangements increased from 57 percent to 65 percent (Figure 2, panel 3). In jurisdictions where the central bank and supervisory authority are separate institutions, an overwhelming 89 percent conveyed in the 2023 survey that they have formalized coordination between them, including information sharing for financial stability purposes.

Figure 2. Governance and Strategy



Source: Survey responses.

Observations and Recommendations

Focused work is needed to develop national-level and financial sector–level cybersecurity strategies. Governance arrangements need improvement in several jurisdictions.

National and financial sector–focused cybersecurity strategies have gained prominence, and more jurisdictions have developed such strategies, but progress is slow, and gaps persist. The majority of countries that responded to either survey had neither a national nor a financial sector cybersecurity strategy, although progress in developing such strategies is notable.

Developing cybersecurity strategies helps in understanding the threat landscape and the levels of national and financial sector preparedness and gaps, thereby providing insight into priorities for action.[3] Guidance for developing a national cybersecurity strategy is widely available and also has been articulated in the guide developed by 20 partners from intergovernmental and international organizations, the private

[3] The National Cybersecurity Strategy repository maintained by the International Telecom Union (https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx) provides information on countries having national strategies and links to documents. The national and financial sector cybersecurity strategies are also published by several countries.

sector, academia, and civil society organizations (NCS 2021). Establishing and maintaining a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines is the first element published by the G7 in its fundamental elements for cybersecurity of the financial sector (G7 2017b). Such strategies, when formulated in a manner consistent with local conditions, implemented by agencies accountable for them, and reviewed periodically, will contribute to strengthening the cybersecurity of the country and the sector.

Successful implementation requires consideration of strategic, political, operational, and technical governance arrangements (ENISA 2023). Governance plays a very important role in ensuring cybersecurity at both national and sectoral levels. Effective governance includes well-thought-out structures; institutional arrangements with clear mandates and allocation of appropriate and adequate legal powers and accountability frameworks; ensuring adequate human, financial, and technical resources; and effective monitoring and follow-up. Governance arrangements are well covered in SSBs' work on operational resilience, cyber resilience, and operational risk management, for example, BCBS (2021a), covering its Principles for Operational Resilience and Principles for the Sound Management of Operational Risk, and CPMI-IOSCO (2016).

It is very important for financial sector regulators to coordinate their activities. In the face of perpetrators of cyberattacks coordinating and leveraging each other's skills, it is increasingly important for financial sector regulators and other stakeholders to also coordinate to counter the threats. Coordination between central banks and supervisory authorities was formalized, including with respect to the sharing of information for financial stability purposes, in close to 90 percent of reporting jurisdictions. The aim should be to achieve convergence in regulations, share best supervisory practices, tackle cyber incidents collectively where required, and share information on a regular basis. Memorandums of understanding between financial regulators help in formalizing common institutional arrangements, such as financial stability committees, financial stability and development councils, and councils of financial regulators.

B. Cyber Regulation and Supervision

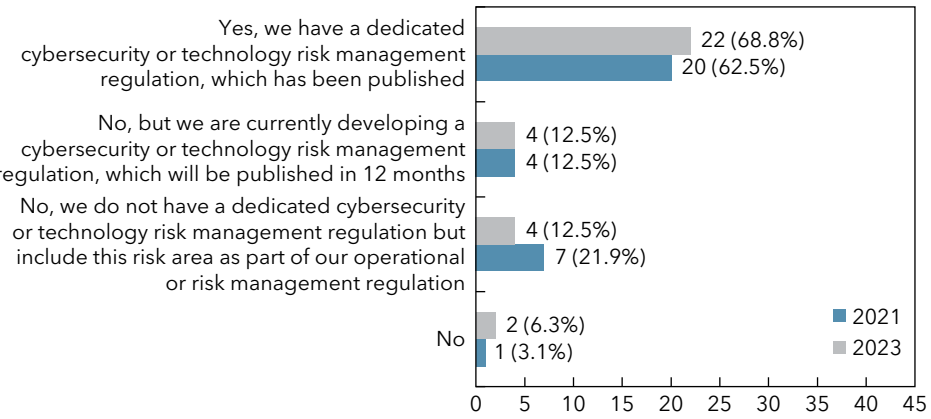
Survey Results

The second theme has eight questions focused on cyber regulation and supervision. The theme covers the availability of dedicated technology and cyber risk regulation, scope of application, availability of data privacy regulation, supervisory architecture, how supervisory concerns on cyber risk are conveyed, methods of on-site supervision, arrangements for off-site supervision, and capacity to conduct on-site examination of third-party service providers.

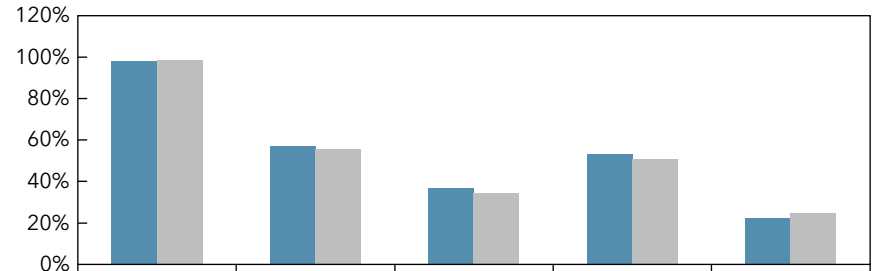
Over the past two survey periods, there has been an increase in the share of jurisdictions reporting dedicated technology or cybersecurity frameworks among countries responding to both surveys (Figure 3, panel 1). Considering all the responses received, more than half of the jurisdictions surveyed in both 2023 and 2021 indicated that they have a dedicated technology or cybersecurity regulation in place, and the number of such countries went up from 29 in 2021 to 38 in 2023, with a small increase in jurisdictions that indicated they would be developing such regulation within a year, from 9 to 12. In the absence of dedicated regulation, a greater number of respondents mentioned that rules are included in other regulatory frameworks. A small minority (7 percent) indicated that they do not have any regulations related to cybersecurity at all. A sector-level analysis reveals that almost all countries report having relevant regulations applicable to banks, over half in relation to financial market infrastructures (FMIs) and nonbanks, about a third in relation to insurance companies, and a quarter in relation to third-party providers (Figure 3, panel 2).

Figure 3. Cyber Regulation—Availability and Applicability

1. Does Your Jurisdiction Have a Dedicated and Published Cybersecurity or Technology Risk Management Regulation for the Financial Sector? (Comparable Data)



2. Applicability of Regulations (Considering All Responses)



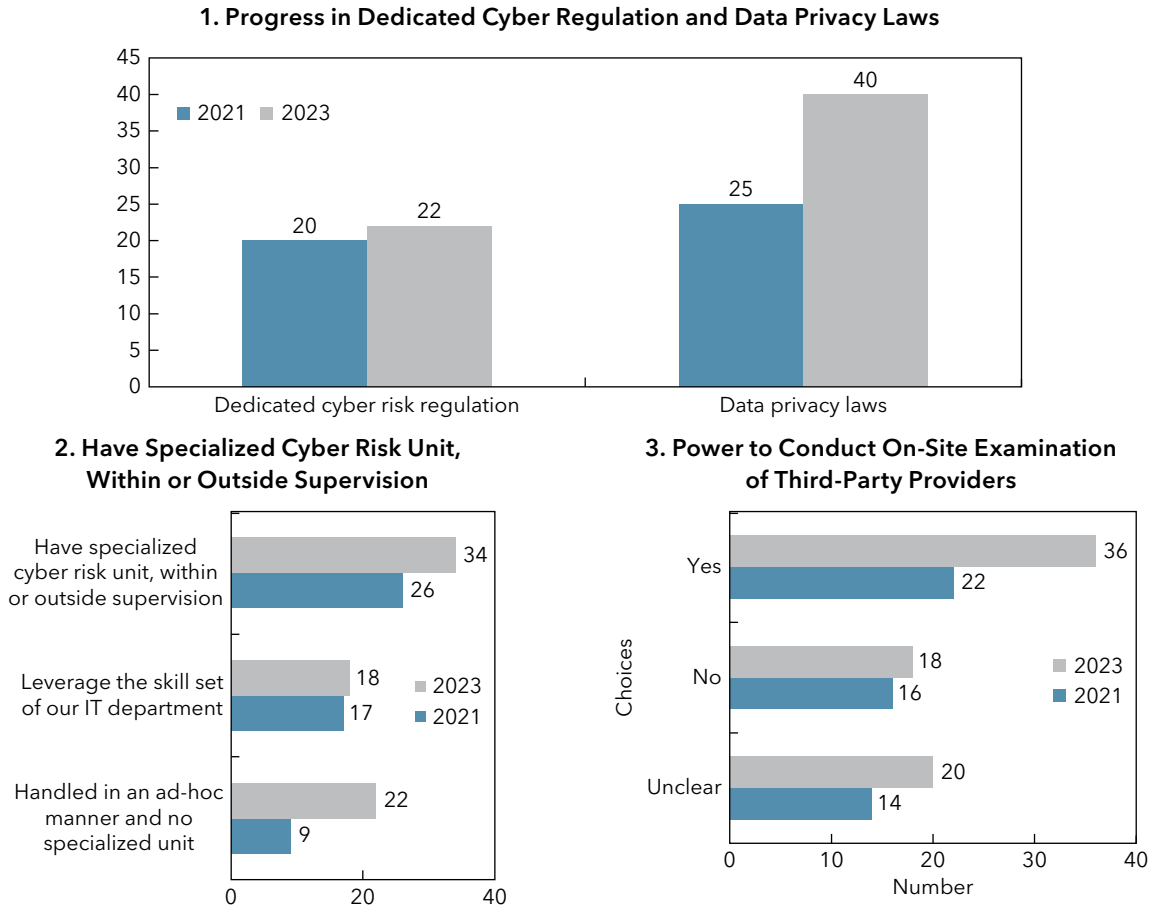
	Banks	FMIs	Insurance companies	Nonbanks	Third-party providers
2021	98%	57%	37%	53%	22%
2023	98%	56%	34%	51%	25%

Source: Survey responses.
Note: FMIs = financial market infrastructures.

Survey results indicate a high degree of correlation between the existence of a national cybersecurity strategy and cyber risk regulation. This suggests that the presence of cybersecurity strategies greatly facilitates establishing cyber risk regulation.

There is an increase in the prevalence of data privacy laws and strengthening of the supervisory architecture among all respondents (Figure 4). Jurisdictions without data privacy laws fell from 38 percent to 28 percent considering all responses, and from 41 percent to 25 percent considering comparable responses. In terms of supervisory architecture, based on 2023 data, 46 percent of jurisdictions had a specialized cyber risk supervision unit, 24 percent leveraged the skills available in their IT departments, whereas 30 percent handled this work in an ad hoc manner. Among low-income countries, instances of having a specialized cyber risk supervision unit were much lower, as is the case in FCS. About a quarter of jurisdictions do not issue an ICT/cyber examination report to their supervised entities.

Figure 4. Cyber Regulation and Supervision (All Responses)



Source: Survey responses.

More than a quarter of surveyed jurisdictions do not conduct on-site examinations covering cyber risk. The share of jurisdictions applying the full range of supervisory approaches, including full scope, limited scope, and thematic reviews plus conducting on-site examinations accounted for about a half in 2021 and 2023. For off-site supervision practices, 43.2 percent indicated that they collect a full range of off-site information and carry out analysis (compared with 35.8 percent in 2021). Conversely, jurisdictions that either had very limited capacity or did not have the capacity to collect off-site information fell from 49 to 37.9 percent during the same period.

The scope of legal supervisory powers has increased vis-à-vis third-party service providers with around half of the respondents, indicating in 2023 that they have legal powers to conduct on-site examinations. Forty-nine percent of surveyed jurisdictions indicated that they enjoy powers to conduct such examinations, and 24.3 percent (30.8 percent in 2021) said that they do not have powers to do so.

Observations and Recommendations

Regulation and supervision of cybersecurity risk is the core component in strengthening the cybersecurity of the financial sector. Legal and regulatory clarity regarding supervisory powers and greater top management attention will contribute to addressing critical gaps. Building regulatory and supervisory capacity to cope

with increased cybersecurity risks is an urgent priority that will be supported through an augmentation of resources. A targeted approach, based on identified gaps, would yield better results. Resource constraints could be contributing to suboptimal progress in establishing a supervisory framework for such risks. The IMF's cyber risk supervision toolkit could be leveraged to speed up capacity-building initiatives.

There is progress in issuing dedicated ICT and cyber risk regulations as well as data privacy laws, but significant gaps persist. The applicability of cyber risk regulations is predominantly directed toward banks, followed by FMIs and other nonbanks. Extending their applicability across the entire financial sector should be a priority. The ongoing work of financial sector standard setters may be used, and that of international standard setters such as the International Organization for Standardization, the National Institute of Standards and Technology, and the Information Systems Audit and Control Association leveraged in framing such regulations. Another useful resource is the Cyber Risk Institute whose Cyber Risk Institute Profile is a cybersecurity framework developed by, and for, the financial sector based on globally recognized standards (see https://cyberriskinstitute.org). Regulatory standards issued by some jurisdictions also provide useful insights into the key components of regulation, such as the European Banking Authority's Guidelines on ICT and security risk management (EBA 2019), the Monetary Authority of Singapore's Technology Risk Management Guidelines, and the Canadian Office of the Superintendent of Financial Institution's Technology Risk Management Guideline.[4] It is important to consider the local environment while framing the regulations to make them suitable for adoption.

Cyber risk supervision needs to be strengthened by increasing the capacity to conduct on-site examinations and off-site supervision beyond current levels. Less than half of the respondents have a specialized cyber risk supervisory unit, suggesting a lesser focus on cyber risk in a majority of reporting jurisdictions. About one-third handled this work in an ad hoc manner. On-site examinations of cyber risk are not carried out by more than one-fourth of the respondents. There is notable progress in extending off-site supervision to cyber risk, but close to 40 percent of respondents did not have, or had at best, limited capacity to collect off-site information.

Third-party risk management has assumed significance, and standard setters as well as major regulators have strengthened their guidelines and regulations. There is progress in extending on-site examinations to third-party service providers. More than one-fourth of the reporting countries are not clear about their legal ability to conduct such examinations. IOSCO's Principles on Outsourcing provide guidance on managing outsourcing risks (see https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf). The FSB has recently published a toolkit for enhancing third-party risk management and oversight (FSB 2023a) which also provides useful insights.

C. Monitoring, Response, and Recovery

Survey Results

The theme on monitoring, response, and recovery has five questions, covering how supervisors are kept informed on the cybersecurity threat landscape, what information they use to understand the threat landscape, whether any revision in regulation was made after the occurrence of a major cyber incident, how supervisors dealt with cyber incidents at supervised entities, and what are their approaches regarding cyber exercises and testing.

[4] For the Monetary Authority of Singapore's Technology Risk Management Guidelines, see https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf. For the Canadian Office of the Superintendent of Financial Institution's Technology Risk Management Guideline, see https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/technology-cyber-risk-management.

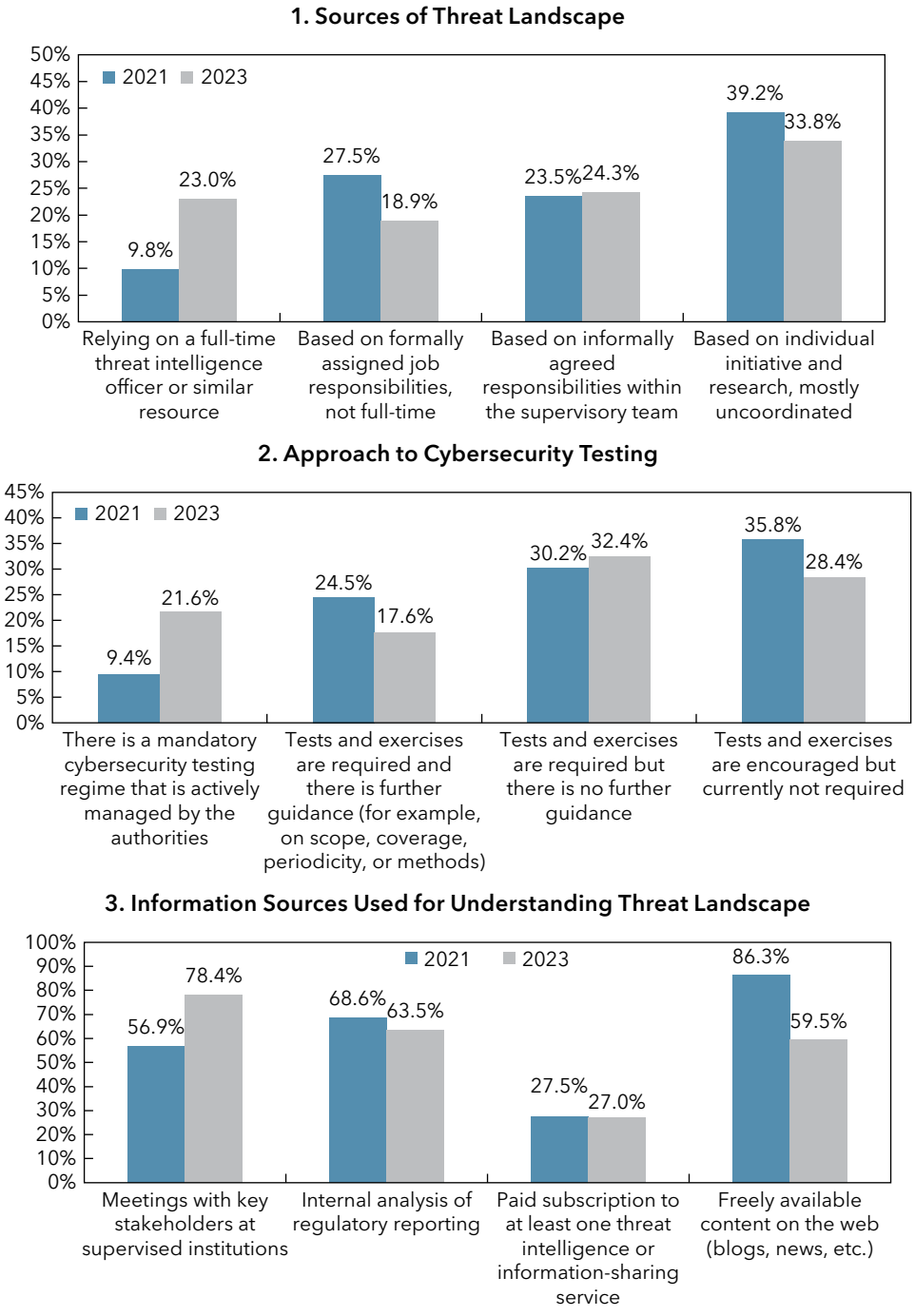
Threat intelligence gathering within central banks and supervisory agencies continues to be based predominantly on informal arrangements and individual initiatives (Figure 5, panel 1—considering all responses). Formal arrangements to collect threat intelligence, either through full- or part-time roles, increased from 37.3 to 41.9 percent. In terms of information sources used to gather threat intelligence, dependence on freely available content fell from 86.3 to 59.5 percent, whereas meetings with key stakeholders at supervised institutions increased from 56.9 to 78.4 percent (Figure 5, panel 3). About a quarter of respondents have paid subscriptions. Internal analysis of regulatory reporting marginally increased during the period.

A significant number of jurisdictions amended cyber regulations after experiencing a major cyber incident, and analyzing mandatory reporting of cyber incidents helped authorities deal with cyber incidents. Forty-four percent of the respondents stated that they amended cyber regulations after a major cyber incident (41 percent in 2021, an increase of 3 percent). In terms of dealing with cyber incidents at supervised entities, 29.7 percent had not established any processes by 2023. Others predominantly use off-site monitoring (60.8 percent) and analysis of reported incidents (52.7 percent), followed by on-site interventions (33.8 percent) in dealing with cyber incidents.

Cybersecurity testing and exercises play an important role in ensuring cybersecurity, but significant gaps persist (Figure 5, panel 2). Results show that authorities mandating a cybersecurity testing regime and actively managing it have moved up from 9.4 percent in 2021 to 21.6 percent in 2023. Conversely, there was a sizable fall in respondents that did not have such a testing regime. About one-third have mandated such tests and exercises without providing any further guidance.

The main source of information gathering with respect to threat intelligence is meetings with key stakeholders in supervised entities, followed by internal analysis of regulatory reporting and freely available online content (Figure 5, panel 3). Paid subscriptions to gather threat intelligence were resorted to significantly less, by about one-fourth of the respondents. Dependence on freely available content noticeably decreased during the period.

Figure 5. Monitoring, Response, and Recovery



Source: Survey responses.

Observations and Recommendations

Central banks and supervisory agencies need to develop processes to understand the threat landscape on an ongoing basis. With significant gaps in terms of response and recovery capabilities after cyber incidents

and low appetite for conducting cyber exercises and tests, cybersecurity preparedness appears weak among emerging market and developing economies. Capacity needs to be augmented in this important area, with focused work on conducting cyber exercises and tests, to help build sectorwide incident response capabilities.

Threat intelligence gathering within central banks and supervisory authorities continues to be based predominantly on informal arrangements and individual initiatives for most survey respondents. In the absence of a clearly articulated threat landscape affecting the financial sector, the response from central banks and supervisors often lacks focus and intensity. Threat intelligence facilitates appropriate measures relating to protection, detection, response, and recovery.

Close to a third of all respondents are yet to establish protocols to handle major cyber incidents in their financial sector. Approaches vary with more jurisdictions tending to favor off-site monitoring tools as compared with on-site intervention, after a major cyber incident.

Cyber exercises and tests play an important role in strengthening response and recovery capabilities. Most respondents either do not require cyber exercises and tests or, when required, do not provide adequate guidance. Only a fourth of surveyed countries mandate cyber exercises and tests and actively manage them. Threat intelligence-based testing exercises have gained momentum, and several jurisdictions mandate such testing for their financial institutions and FMIs—for example, European framework for Threat Intelligence-based Ethical Red-Teaming (TIBER-EU), a targeted assessment that allows regulators and firms to better understand weaknesses and vulnerabilities and take remedial actions (CBEST) (Bank of England), the Intelligence-led Cyber Attack Simulation Testing (iCAST) (Hong Kong Monetary Authority).[5] Though such advanced arrangements offer greater benefits, they require a minimum level of preparedness of the supervisor as well as the supervised institutions and often tend to be elaborate, expensive, and requiring a wide range of skills. In emerging market and developing economies, such arrangements typically cover vulnerability scans and penetration testing (examples include Ghana, India, Nigeria, and Philippines).

The FSB's "Effective Practices for Cyber Incident Response and Recovery" (FSB 2020) provides useful guidance to strengthen response and recovery capabilities. The cyber incident response and recovery practices cover all organizations in the financial ecosystem because the financial system is only as strong as its weakest link. Therefore, organizations and authorities must collectively strengthen their capabilities through frequent engagements in information sharing, exchanges of best practices, and cyber-related exercises. The cybersecurity framework of the National Institute of Standards and Technology comprises five functions, of which response and recovery functions focus on (1) appropriate activities to take regarding a detected cybersecurity incident and the ability to contain the impact of a potential cybersecurity incident, (2) appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cybersecurity incident, and (3) timely recovery to normal operations to reduce the adverse impact of a cybersecurity incident. The CPMI-IOSCO cyber resilience guidelines also address the response and recovery aspects in some detail. These standard setters' work can be leveraged by jurisdictions to strengthen their capabilities.

D. Information Sharing and Incident Reporting

Survey Results

The theme on information sharing and incident reporting has 10 questions, covering the availability of information-sharing arrangements in the financial sector, membership in such forums, arrangements with financial

[5] For TIBER-EU, see https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf. For CBEST, see https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide.

authorities in other countries and with other sectors; availability of an incident reporting regime; taxonomy and categorization of the severity of incidents; materiality thresholds; availability of reporting templates; and how wholesale payment systems leverage existing arrangements to strengthen cybersecurity.

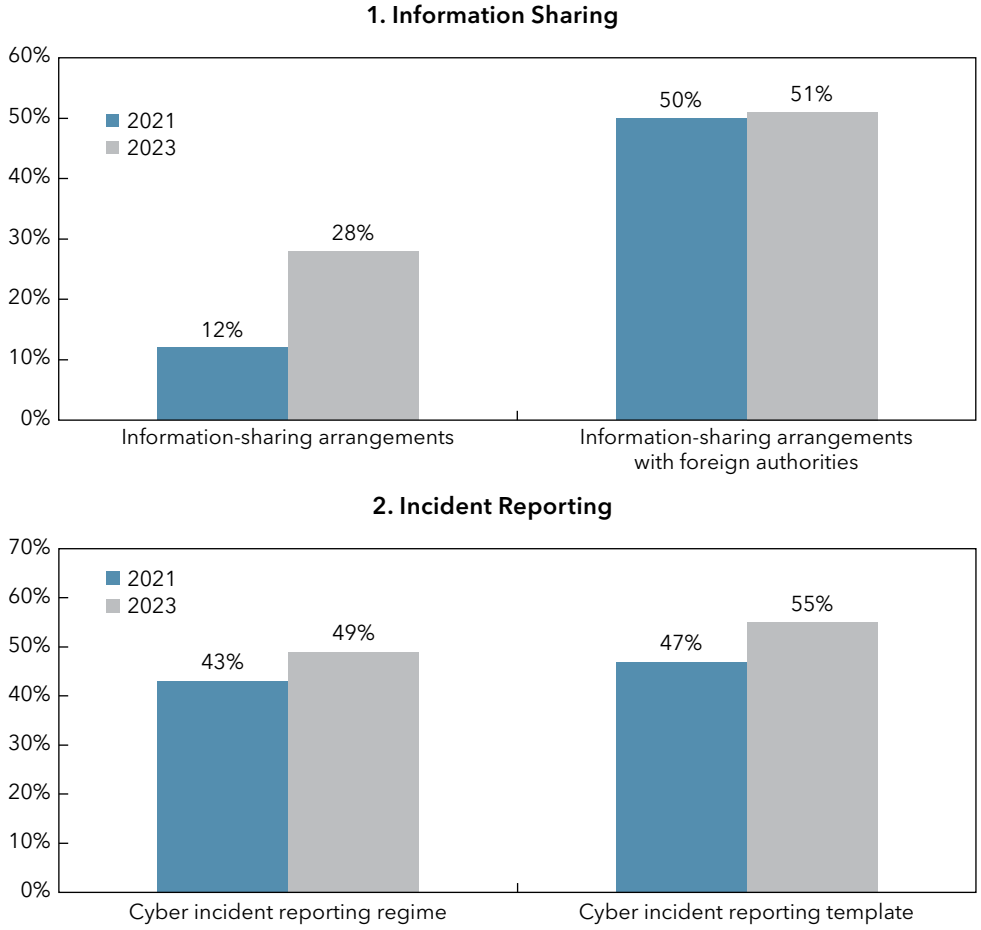
Respondents confirming systematic information-sharing arrangements within the financial sector rose from just over 12 percent to almost 28½ percent (Figure 6, panel 1).[6] Half of the respondents indicated that they are part of information-sharing arrangements with foreign financial sector authorities as well as sectoral authorities within their own country.

By 2023, about half of the respondents had an incident reporting regime, a small increase relative to 2021 (Figure 6, panel 2). The share of jurisdictions having a cyber incident reporting regime went up from 43 percent to 49 percent between the two surveys. The share of jurisdictions having a cyber incident reporting template moved up from 47 percent to 55 percent, suggesting that a few jurisdictions have prescribed a cyber incident reporting template even when they did not have a cyber incident reporting regime. A smaller proportion of respondents noted that these incidents are reported in line with existing guidelines for operational risk management. Eleven percent of respondents had no such arrangements in place, a similar number to 2021, and a taxonomy/severity classification of cyber incidents was not in place in 53 percent of the respondents, with very little change between the two surveys. Among jurisdictions with incident reporting regimes, 41 percent did not have an established methodology to assess the impact and severity of the cyber incidents.

Wholesale payment systems and messaging networks are becoming an integral part of cybersecurity preparedness. Of the respondents, 59.5 percent mentioned that wholesale payment systems and messaging networks are part of information-sharing networks and collaborate toward building cyber awareness, an increase relative to 2021 when it was just under a half. Also, 54.1 percent (39.6 percent in 2021) said that wholesale payment systems and messaging networks leveraged existing cybersecurity working groups for implementing fraud prevention strategy.

6 Almost 40 percent of respondents indicated that they are not aware of information-sharing arrangements.

Figure 6. Information Sharing and Incident Reporting



Source: Survey responses.

Observations and Recommendations

Significant work needs to be undertaken to help design and develop information-sharing networks within the financial sector, as well as with other sectors and overseas financial sector regulators. Cyber incident reporting frameworks, including templates, defined thresholds, appropriate taxonomy, and criteria for severity classifications, need to be a top priority for jurisdictions.

Despite the perceived significant benefits of tackling cyberattacks, information sharing is not prevalent in about three-quarters of the respondents. Information sharing among good actors assumes further significance in the light of extensive coordination and cooperation among bad actors targeting the financial sector. Strategic, operational, and tactical information as well as threat intelligence are shared under such arrangements, which can be multidirectional, that is, regulators to regulators, regulators to financial sector participants, financial sector participants to regulators, and among financial sector participants without the involvement of the regulators. Surveys suggest that authorities themselves need to do more because only half of them are part of such information-sharing networks. Corresponding arrangements with foreign financial authorities and other sectors within the country also exhibit gaps.

In making progress in this important area, reporting jurisdictions may draw lessons from existing arrangements, including any of the following:

- One of the major initiatives in this regard is the Euro Cyber Resilience Board's Cyber Information and Intelligence Sharing Initiative. It brings together a community of public and private entities with the aim of sharing intelligence and exchanging best practices. The core objectives of the initiative are to protect the financial system by preventing, detecting, and responding to cyberattacks; to facilitate the sharing of information, intelligence, and best practices among financial infrastructures; and to raise awareness of cybersecurity threats.
- The Financial Services Information Sharing and Analysis Center is a global cyber intelligence sharing community focused on financial services.
- CISP (Connect, Inform, Share, Protect) is a platform for cybersecurity professionals in the United Kingdom to collaborate on cyber threat information in a secure and confidential environment.

Similar arrangements are in place in many advanced economies. It is important for all jurisdictions to take initiatives to facilitate information sharing in a proportionate way.

A cyber incident reporting regime is vital to strengthening the cybersecurity of the financial sector. The FSB's "Final Report on Recommendations to Achieve Greater Convergence in Cyber Incident Reporting" (FSB 2023b) sets out actions and steps that authorities can take to promote convergence among cyber incident reporting frameworks and encourage better practices. The report also sets out a concept for developing a common format for incident reporting exchange (see https://www.fsb.org/wp-content/uploads/P130423-2.pdf), to collect incident information from financial institutions that authorities could use for information sharing. Institutionalizing a cyber incident reporting regime should be a high priority for all jurisdictions.

There is further scope for wholesale payments and messaging networks to leverage existing cybersecurity working groups and be part of information-sharing networks. The CPMI has published a toolkit (CPMI-IOSCO 2019) for reducing the risk of wholesale payments fraud related to endpoint security, which can be leveraged to improve the security. The Society for Worldwide Interbank Financial Telecommunication (SWIFT)'s customer security program (see https://www.swift.com/myswift/customer-security-programme-csp) is aimed at ensuring that financial institutions improve their defense against cyberattacks and contribute to protecting the integrity of the wider financial network.

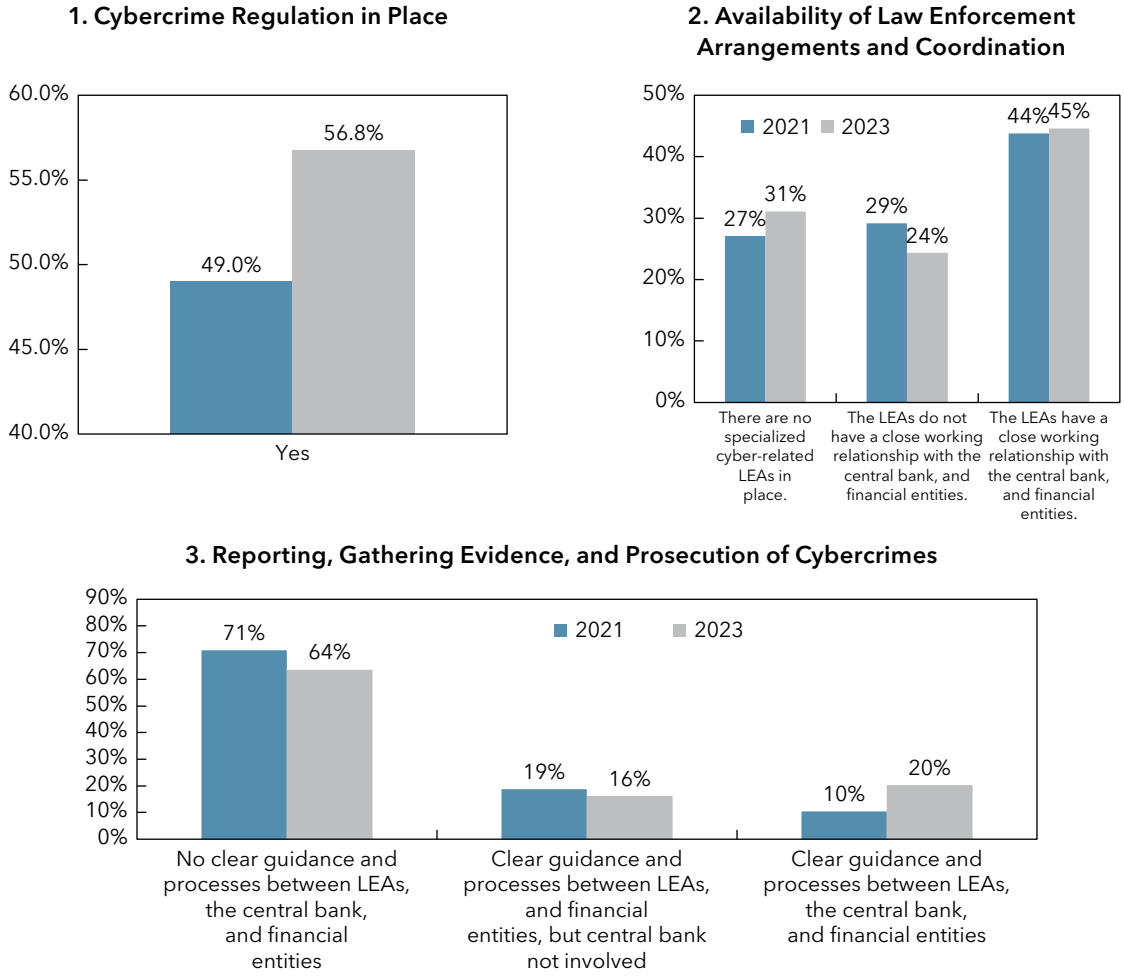
E. Cyber Deterrence

Survey Results

The theme on cyber deterrence has four questions, covering the existence of cybercrime laws and regulations; the role of law enforcement authorities (LEAs) in dealing with cyber incidents; the relationship among LEAs, central banks, supervisory authorities, and financial sector entities; and the coordination between the CERT and financial supervisory authorities.

Most jurisdictions had cybercrime regulation in place (Figure 7, panel 1). These regulations set out the types of cybercrime, the roles and responsibilities of LEAs, the processes for prosecuting cybercriminals, and the punishment to be meted out to such criminals. A total of 44.6 percent of the respondents (43.8 percent in 2021) indicated that LEAs have specialized cyber units and are responsible for combating, preventing, disrupting, investigating, and prosecuting cybercrime and cybercriminals and have a close working relationship with the central bank and financial entities (Figure 7, panel 2). However, a significant majority of jurisdictions (63.5 percent in 2023) continued to note the absence of clear guidance and processes for LEAs, central banks, and financial entities on the reporting of cybercrimes, for retaining digital evidence, and for transferring this evidence to aid prosecution of cybercriminals (Figure 7, panel 3).

Figure 7. Cyber Deterrence



Source: Survey responses.
Note: LEAs = law enforcement authorities.

Almost a third of respondents have no CERTs in their countries. Even for those countries where CERTs are present, 17.6 percent of all respondents indicated that there is no coordination between the supervisory authorities and the CERT, a result similar to that in the 2021 survey. An additional 28.4 percent of countries that report good coordination do not have FinCERT.[7] Among countries that reported having a FinCERT in 2023, the central bank ran this agency in almost 59 percent of these jurisdictions.

Observations and Recommendations

Institutional arrangements in terms of enabling legal provisions to criminalize cyberattacks and establish CERT/FinCERT need special attention. Where such arrangements are available, coordination among all the stakeholders needs to be developed and maintained.

There is a lack of clarity on how to report cybercrime, retain digital evidence, and transfer this evidence to aid prosecution of cybercriminals. Cybercrime regulation needs to set out the different types of cybercrime,

[7] CERTs focused on the financial sector are called FinCERTs.

the roles and responsibilities of LEAs, the processes for prosecuting cybercriminals, and the punishment to be meted out to such criminals. These are often enshrined in cybersecurity or similar laws. Fifty-seven percent of respondents mentioned that they do have cybercrime regulations in place, a notable increase compared with 2021, although more than two-thirds of reporting countries are yet to issue clear guidance for, and processes between LEAs, central banks, and financial sector entities.

CERTs have become a standard arrangement across countries to deter and respond to cyber incidents, but coordination between the CERT and central bank leaves scope for improvement. The survey highlighted that two-thirds of responding jurisdictions have a CERT, albeit even where CERTs are functional, the coordination between them and the central bank varies across jurisdictions. In this context, a report published by International Telecommunication Union, "ITU Cybersecurity Program: CIRT Framework" sets out helpful guidance for jurisdictions in establishing a national CERT and outlines cooperation mechanisms at the regional and international levels that identify, manage, and respond to cyber threats (see https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYBERSEC-2021-01-PDF-E.pdf).

F. Financial Stability Analysis

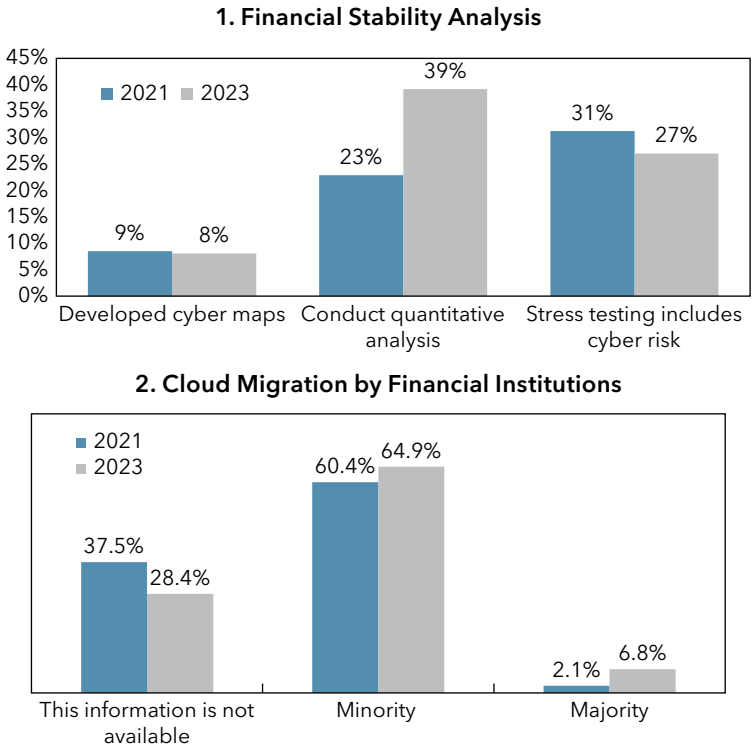
Survey Results

The theme on financial stability analysis has four questions, covering the availability of capacity to develop cyber maps; quantitative analysis of cyber risk; inclusion of cyber risk in stress testing programs; and awareness regarding cloud migration by the financial sector.

"Cyber maps" assist in strengthening cybersecurity, but only 8 percent of respondents had one by 2023 (Figure 8, panel 1). Cyber maps identify the main technologies, services, and connections between financial sector institutions, service providers, and in-house or third-party systems. Sixty percent of the respondents indicated that they were not in possession of the required information to develop such maps. About 31 percent of respondents said that they are in the process of developing one and are expecting to complete the work within the next 12 months.

The majority of respondents do not carry out quantitative analysis or factor cyber risk in stress tests (Figure 8, panel 1). A total of 39.2 percent of respondents said that they collect data on frequency and loss arising from cyberattacks and carry out such analysis, a significant jump up from 23 percent of respondents in 2021. Three-fourths of the respondents said they do not include cyber risk as part of their stress test program.

Figure 8. Financial Stability Analysis



Source: Survey responses.

Key information on the financial sector's cloud migration is not available to supervisory authorities and central banks, although by 2023, the monitoring status has improved relative to two years earlier (Figure 8, panel 2). In 2023, 28.4 percent of respondents said that they did not have any information. The question also sought answers regarding the extent of such migration with responses indicating that in 60.4 percent of countries, a small share ("minority") of financial institutions had migrated and only 6.8 percent of countries had a majority of financial institutions migrated.

Observations and Recommendations

Efforts are needed to develop cyber mapping, which will help in strengthening cybersecurity. Data collection efforts need to be augmented to facilitate financial stability analysis and to be better informed of the digital landscape and dependency on third-party providers.

The survey findings reveal that cyber risk is not widely considered part of financial stability analysis, irrespective of whether it is quantitative analysis or stress testing. This is a material gap in view of the fact that a significant cyber incident, if not properly contained, could seriously disrupt the functioning of the financial system, including critical financial infrastructure, which will have broader financial stability implications. There is a growing realization that cyber risks may, in certain circumstances, pose financial stability concerns and, hence, need to be a part of financial stability analysis despite challenges like data availability, quantification, and unique characteristics, such as interconnectedness, borderless attackers, and potential for contagion. There are two types of stress testing. One type estimates the financial impact of a major cyber incident under a severe but plausible scenario (in terms of the impacts on liquidity and solvency of firms). Analysis in which a severe cyber incident is considered one of the scenarios is becoming prevalent in stress

tests that estimate liquidity and capital requirements. The other type of stress test focuses on the resilience of institutions to respond to, and recover from, cyber incidents and is referred to as a cyber resilience stress test, of which examples include the Bank of England's cyber stress test and the European Central Bank's cyber resilience stress test.[8]

Cyber mapping as a tool is still underdeveloped and under development in most jurisdictions. The Principles for Operational Resilience of BCBS highlight mapping interconnections and interdependencies as a separate principle and set out the expectation that the respective critical functions should map (that is, identify and document) the people, technology, processes, information, facilities, and the interconnections and interdependencies among them as needed to deliver the bank's critical operations. These include those dependent on, but not limited to, third parties or intragroup arrangements. Cyber mapping could be very useful in understanding vulnerabilities, identifying critical nodes, facilitating enhanced oversight of these critical nodes, and achieving better risk management results and communication with stakeholders including the boards.

Despite notable progress in cloud adoption by the financial sector, up to a third of respondents did not collect information on cloud migration. Where collected, it was seen as having gained momentum, with third-party dependencies on the rise on the back of increased digitalization of the financial sector. The pace of cloud adoption has accelerated across all jurisdictions. Many financial sector regulators have recognized this and have issued focused regulation on adoption of cloud by financial sector participants. Recognizing the importance of these issues, the FSB issued a paper on "Third-Party Dependencies in Cloud Services—Considerations on Financial Stability Implications" (FSB 2019).

G. Continuous Learning and Capacity Development

Survey Results

The theme on continuous learning and capacity development has five questions, covering the approach to strengthen cyber risk supervisory capacity; approaches to build cyber risk awareness; training options available; requirement of an IT training and qualification for the supervisor; and the requirement of professional certifications for supervisory staff.

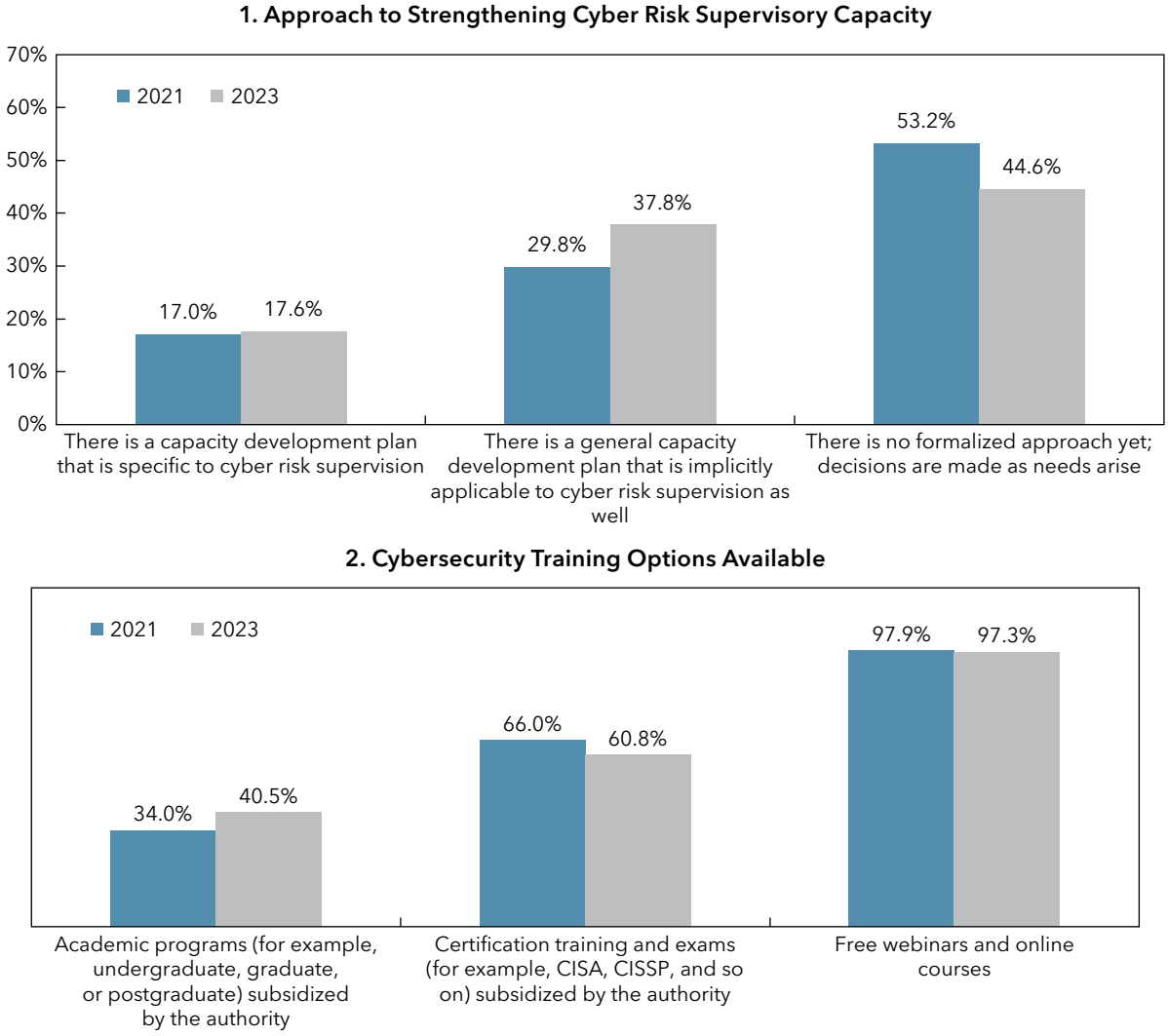
Building supervisory capacity and awareness ought to be priorities. In building this capacity, 17.6 percent of authorities mentioned that they had a specific plan for cybersecurity capacity development, 37.8 percent mentioned that these requirements are covered under general supervisory capacity development initiatives, and the remaining 44.6 percent did not have a plan for supervisory capacity development (Figure 9, panel 1). In building awareness, authorities predominantly used workshops with key stakeholders (78.4 in 2023), followed by interviews, speeches, and publications (60.8 percent). All the categories of continuous learning and capacity development recorded an increase highlighting the attention of the authorities. Participating in and encouraging public–private partnerships moved up from 37 percent to 56.8 percent during the period between 2021 and 2023, with cooperation with academia being the least preferred method (27 percent).

Training options explored varied among jurisdictions (Figure 9, panel 2). In terms of training options, the questionnaire sought to understand the use of (1) free webinars and online courses, (2) certification training and exams subsidized by the authority, and (3) academic programs subsidized by the authority. Over 97 percent of respondents mentioned that they use free webinars and online courses. Certification training and exams stood at second place with over 60 percent using it, followed by academic programs at about 40 percent.

[8] For the Bank of England's cyber stress test, see https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2023/thematic-findings-2022-cyber-stress-test.pdf. For the European Central Bank's cyber resilience stress test, see https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240103~a26e1930b0.en.html.

Technical qualifications required of supervisory staff contribute to addressing skill gaps. In the 2023 survey, over 60 percent of respondents indicated that they require an IT degree for cybersecurity supervisory staff; 32.4 percent indicated that professional certification requirements are required for all cyber risk supervisors; and 28.4 percent indicated that such requirements are only present for senior supervisors. There was no professional certification requirement for 39 percent of the respondents.

Figure 9. Continuous Learning and Capacity Development



Source: Survey responses.

Note: CISA = Certified Information System Auditor; CISSP = Certified Information Systems Security Professional.

Observations and Recommendations

Building cybersecurity supervisory capacity requires more attention in most jurisdictions. Resource constraints compel most to avail themselves of free webinars and online courses for capacity building, but requiring professional certifications and academic qualifications is now gaining momentum across emerging market and developing economies.

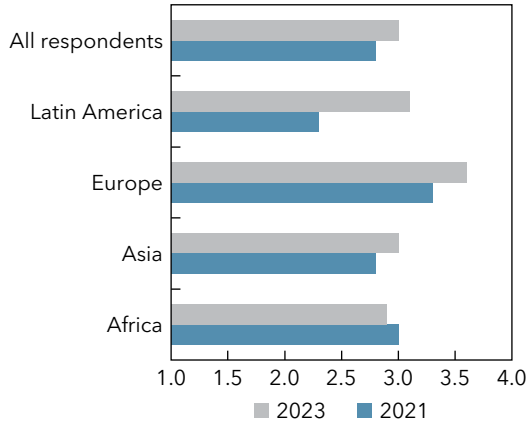
Gaps in capacity building demonstrate the desirability of the IMF playing a proactive role. The online course on cyber risk supervision could be used as a blended learning tool more often; the cyber risk supervision toolkit may be leveraged to further hasten capacity-building efforts, and long-term plans to develop capacity in jurisdictions should be considered.

V. A Cybersecurity Preparedness Index

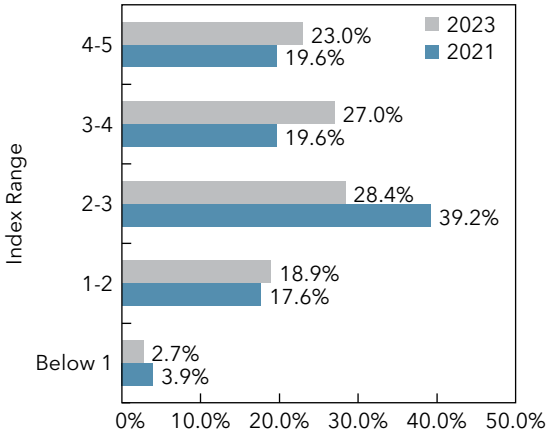
A CPI has been developed using the survey data, providing a summary view of cybersecurity preparedness and trends therein (Figure 10). Of the 42 questions in the survey, 15 are considered more reflective of cybersecurity preparedness. An index is constructed based on this subset of questions. Every question is assigned a score from 0 to 5, where higher scores indicate more favorable outcomes regarding cybersecurity preparedness. The scores are assigned using expert judgment basis. Five of the 15 questions used in the construction of the CPI are considered foundational requirements, and hence, a higher weight of 10 percent is assigned to them, whereas each of the remaining 10 questions is assigned a weight of 5 percent. Details of the methodology are given in Annex 3.

Figure 10. Survey Index

1. Cybersecurity Index–Regional Behavior



2. Cybersecurity Index–Distribution



Sources: Survey responses; and IMF staff calcuations.

Overall, the CPI score improved marginally from 2.8 to 3.0 between 2021 and 2023, with material regional variation. Among regions, Europe did relatively well, with scores improving from 3.3 to 3.6; the Latin American region improved its score the most from 2.3 to 3.1; and African and Asian countries both have scores below 3 for both the surveys. Looking at the set of countries that responded to both the surveys, the scores improved from 2.9 to 3.3. The scores are the lowest for countries with the lowest income levels, and scores for FCS countries are lower than those of non-FCS countries.

An analysis of the distribution of CPI scores indicates that a large share of respondents has progressed to a higher range of scores. Close to one-fourth of the respondents have a score of 4–5, compared with one-fifth earlier. Similarly, 27 percent of the respondents had a score of 3–4 in 2023, compared with one-fifth in 2021. Those who score above 3—indicating a reasonable level of preparedness—rose to 50 from 40 percent earlier. Respondents scoring 2 or less remained more or less at the same level of about one-fifth.

VI. Conclusions

Cybersecurity is a growing risk in the financial sector and central banks, and supervisory authorities have a key role in managing this risk and ensuring cybersecurity preparedness. Global groups and SSBs have increasingly focused on cybersecurity risk, and their work provides a framework to manage this risk. An understanding of cybersecurity preparedness of central banks and supervisory authorities informs capacity-building initiatives needed to bridge critical gaps.

Responses to the 2021 and 2023 cyber surveys provide insights into the cybersecurity preparedness of central banks and supervisory authorities, underlining the progress made as well as the gaps that remain to be addressed. National and financial sector cybersecurity strategies have gained prominence, and more jurisdictions have developed such strategies, but progress is slow, and gaps persist in areas such as issuing dedicated ICT and cyber risk regulations and data privacy laws; establishing a specialized cyber risk supervisory unit; extending on-site examinations to third-party service providers; formalizing arrangements for threat intelligence gathering within central banks and supervisory authorities; and establishing protocols to handle major cyber incidents in the financial sector. Most of the respondents either do not require cyber exercises and tests or, when required, do not provide any guidance. The survey brought out that one-third of the jurisdictions did not have a CERT to respond to cyber incidents, and where CERTs are functional, the coordination between CERT and the central bank varies across jurisdictions. The survey findings reveal that cyber risk is not considered a part of the financial stability analysis by most of the respondents.

Several recommendations flow from the analysis of survey results. Concerted efforts are needed to develop national and financial sector–focused cybersecurity strategies. Building cyber risk regulatory and supervisory capacity is a priority, and a targeted approach based on identified gaps would yield better results. Resource constraints could be contributing to less-than-optimal progress in establishing a supervisory framework for cyber risk. Legal and regulatory clarity on powers of the supervisors, top management attention, and augmentation of resources will help address the gaps. Central banks and supervisory agencies need to develop processes to understand the threat landscape on an ongoing basis. Capacity needs to be augmented in conducting cyber exercises and tests to help build sectorwide incident response capabilities. Institutional arrangements in terms of enabling legal provision to criminalize cyberattacks and establishment of CERT/FinCERT need special attention. Efforts are needed to develop cyber mapping, which will help strengthen cybersecurity. Cybersecurity supervisory capacity building requires more attention in most jurisdictions. The gaps in capacity building clearly demonstrate the need for the IMF to play a proactive role.

ANNEX 1. Survey Questionnaire

IMF Cybersecurity Questionnaire – 2021 & 2023

Name of central bank or supervisory agency:

Name of jurisdiction:

Completed by:
Role:
Date completed:

What is the deadline for completion/return?
The completed questionnaire should be returned to the IMF within 4 weeks of receipt.

Who should complete the questionnaire?
The questionnaire should be completed by competent parties with appropriate knowledge and experience, specifically in the subject matter of cyber risk supervision and oversight.

How should the central bank or supervisory agency answer if more than one answer applies?
In case more than one answer applies, select all that apply, and you may provide an explanatory note at the end of the survey in the textbox if necessary.

Can any questions be left blank if the central bank or supervisory agency is uncertain of the current position for the jurisdiction?
No. All questions must be answered to the central bank or supervisory agency's best ability.

Will the central bank or supervisory agency need to provide documentation or information that supports the answer selected?
No. This questionnaire is not an assessment of the jurisdiction's cyber capabilities or maturity. The questionnaire aims to collect data on key elements about cybersecurity of the financial sector, to further aid the IMF in developing tools to build capacity globally.

Governance and strategy

Q. No	Question and multiple-choice answers
1	Does your jurisdiction have a national cyber strategy, which includes the financial sector? a) Yes, we have a national cyber strategy, which includes the financial sector. b) No, but we, as the central bank or supervisory agency, are currently working on a government-driven national cyber strategy, that is expected to be endorsed in the next 12 months. c) No, but the government is developing a strategy that is expected to be finalized in the next 12 months (without active involvement of the central bank/supervisors) d) No, we do not have a national cyber strategy, although there are ongoing discussions on whether we should develop such a strategy. e) No.

2	Does your central bank or supervisory agency have a cyber strategy for the financial sector? a) Yes, and it is integrated into the national cyber strategy. b) Yes, however, it is separate and not connected to the national cyber strategy. c) No, but we are currently developing one and expect to publish it within the next 12 months. d) No.
3	Did the Board of your central bank or supervisory agency approve the central bank or supervisory agency's cyber strategy for the financial sector, and does it regularly monitor its progress in implementation? a) Yes. b) No.
4	Does your jurisdiction have formalized governance arrangements in place to manage cyber risk? a) Yes, our jurisdiction has a formalized governance structure in place at government level, which delegates to the central bank and the supervisory agencies the responsibility for mitigating cyber risk in the financial sector. b) Yes, there is a formalized governance structure in place within the central bank and supervisory agencies; however, the governance arrangements are not connected with other governmental agencies and other sectors. c) No, but there is ongoing work at government level expected to be finalized in the next 12 months. d) No, but the central bank/supervisory agency is currently working on establishing formalized governance arrangements within the central bank or supervisory agency in the next 12 months. e) No, not at governmental level nor within the central bank or supervisory agency. If there is ongoing work to develop such arrangements, it is expected to take longer than 12 months.
5	What is the mandate of the central bank or supervisory agency with regard to cyber risk? **(Select all that apply)** a) The central bank/supervisory agency is responsible for cyber risk as part of: • prudential supervision of financial institutions () • oversight of financial market infrastructures () • financial stability () • operation of the RTGS system () • operating the financial CERT or similar activity () • carrying out cyber exercises and coordinating testing frameworks ()
6	The central bank and supervisory agency have a formalized working relationship with each other, which includes sharing of information for financial stability reasons? • Yes () • No () • Not applicable (the central bank is also responsible for supervision)

Cyber regulation and supervision

Q. No	Question and multiple-choice answers
7	Does your jurisdiction have a dedicated and published cybersecurity or technology risk management regulation for the financial sector? a) Yes, we have a dedicated cybersecurity or technology risk management regulation, which has been published. b) No, but we are currently developing a cybersecurity or technology risk management regulation, which will be published in 12 months. c) No, we do not have a dedicated cybersecurity or technology risk management regulation but include this risk area as part of our operational or risk management regulation. d) No.
8	Does your cybersecurity regulation apply to: • Banks () • FMIs () • Insurance companies () • Non banks () • Third party providers () • None of the above, as we do not have cybersecurity regulation () **(Select all that apply)**
9	Does your jurisdiction have a dedicated and published data privacy regulation? a) Yes. b) No, but we are currently developing one, which will be published in 12 months. c) No.
10	How is the supervisory architecture organized within your jurisdiction? a) We have a specialized Cyber Risk Unit as part of the Supervision Department. b) We have a specialized Cyber Risk Unit outside the Supervision Department. c) We leverage the skill set of our IT department to conduct ICT/cyber examinations, but these are coordinated by the Supervision Department. d) We do not have a specialized Cyber Risk Unit as of now, but we are planning to have one soon. We do not take support from the IT Department and ICT/cyber risk work is handled by generalists in an ad hoc manner.
11	How are ICT/cyber risk concerns conveyed to the supervised entity? a) ICT/Cyber risk is part of the Examination Report issued to the supervised entity. b) While major ICT/cyber risk observations are included in the main Examination report, a separate ICT/cyber risk report is issued to the supervised entity. c) ICT/Cyber risk observations are not part of the main Examination report; but an ICT/cyber risk examination report is issued separately to the supervised entity. d) ICT/Cyber risk assessments do not lead to the issue of any report, but major actionable items are conveyed by way of a supervisory letter. e) ICT/cyber risk observations are discussed with the supervised entity but are not conveyed through the Examination Report nor through supervisory letters.

12	What are the methods deployed for on-site supervision of cyber risk? a) We have a full range of approaches (full scope examination, limited scope examination, short visits and thematic reviews), as well as the legal powers to mandate external audits and forensic investigations. b) We conduct on-site supervision (full scope or limited scope examination). Thematic reviews are generally not used but we have legal powers to mandate external audits or forensic investigations. c) We conduct predominantly thematic reviews. Full scope examinations are rare, but we do limited scope examinations at times. We have legal powers to mandate external audits or forensic investigations. d) We require an external audit of cyber preparedness of banks/FMIs on a yearly basis. We have limited capacity to conduct on-site examinations. e) We do not conduct on-site examinations. We do not have the legal powers to mandate external audits or forensic investigations.
13	What are the arrangements for off-site supervision of cyber risk? a) We collect a full range of off-site information that pertains to ICT/cyber. We carry out analysis of such data with a focus to identify material risks faced by the individual entity as well as the system as a whole, and we provide key inputs to the on-site team. b) We have a separate off-site function which collects data, which we analyze regularly. c) We have just established an off-site function and currently collect very limited information. We plan to strengthen the off-site function significantly in the coming year. d) We do not have a dedicated off-site function, but we have the capability to collect ad hoc information at a short notice. e) At this juncture, we do not have any plan to set up an off-site function for ICT/cyber.
14	Do you have powers to conduct an on-site inspection of third-party providers, if necessary? a) Yes. b) No. c) Unclear.

Monitoring, response and recovery

Q. No	Question and multiple-choice answers
15	How do supervisors keep informed about cybersecurity risks and emerging threats ("threat landscape")? a) Based on individual initiative and research, mostly uncoordinated. b) Based on informally agreed responsibilities within the supervisory team. c) Based on formally assigned job responsibilities, not full-time. d) Relying on a full-time threat intelligence officer or similar resource.
16	What information sources do you use to understand the threat landscape? **(Select all that apply)** a) Freely available content on the web (blogs, news, etc.). b) Paid subscription to at least one threat intelligence or information-sharing service. c) Internal analysis of regulatory reporting. d) Meetings with key stakeholders at supervised institutions.

17	Did you publish updates in the past two years to your cybersecurity regulation in response to changes in the threat landscape? a) Yes, specifically in the areas of _____. b) No. c) We don't have specific cybersecurity regulation.
18	How do you deal with cybersecurity incidents occurring at supervised institutions? **(Select all that apply)** a) Analyzing mandatory reporting of cyber incidents. b) Off-site monitoring the response and recovery activities of the institution. c) On-site involvement in response and recovery without taking control (that is, advisory role). d) On-site direction and control of response and recovery activities. e) We have not established the process yet.
19	What is your approach to cybersecurity testing and exercises? (such as penetration tests, red teaming, and effectiveness of cyber incident response and crisis management exercises.) a) Tests and exercises are encouraged but currently not required. b) Tests and exercises are required but there is no further guidance. c) Tests and exercises are required and there is further guidance (for example, on scope, coverage, periodicity, or methods). d) There is a mandatory cybersecurity testing regime that is actively managed by the authorities.

Information sharing and incident reporting

Q. No	Question and multiple-choice answers
20	Do you have a cyber information and intelligence sharing arrangement in place in your financial sector? a) Yes, the financial entities in the sector systematically share information and intelligence with each other. b) No, but all financial entities or most financial entities are part of an information-sharing network, such as Financial Services Information Sharing and Analysis Center (FS-ISAC) c) No, but we are developing an information and intelligence sharing network with the financial sector. This will be operational in the next 12 months. d) No, we are not aware of any such arrangement.
21	Are you, as a central bank or supervisory agency, a member of industry-wide information-sharing groups (for example, national computer emergency response team (CERT), FS-ISAC, or the information-sharing arrangement cited in the question before)? a) Yes. b) No.
22	Does your authority have information-sharing arrangements with financial authorities in other jurisdictions (for example, foreign authorities)? a) Yes. b) No.
23	Does your authority have information-sharing arrangements with authorities across sectors within your jurisdiction? a) Yes. b) No.

24	Do you have a cyber incident reporting regime in place? a) Yes, we have a dedicated cyber incident reporting regime, and financial institutions are required to report incidents by law or regulation. b) No, we don't have a dedicated and specific cyber incident reporting regime in place but financial institutions are required to report incidents as part of their operational risk requirements. c) No.
25	Have you established (a) a taxonomy of cyber incident (to designate them) and (b) a categorization of their severity to measure their importance? a) Yes, both (a) and (b). b) Only (a). c) Only (b). d) No, neither.
25	Indicate which of the following you have established. a) A taxonomy of cyber incident (to designate them). b) A categorization of their severity to measure their importance. c) None of the above.
26	Do you have an established methodology for determining the materiality (that is, the impact and severity) of a cyber incident that is used in cyber incident reporting? a) Yes. b) No. c) Not applicable (do not have a cyber incident reporting framework).
27	Do you issue a cyber incident reporting template to your supervised institutions? a) Yes. b) No. c) Not applicable (do not have a cyber incident reporting framework).
28	Does the operator and participants of a wholesale payment system or a messaging network collaborate in support of information sharing and ongoing education and awareness about evolving endpoint security risks and risk controls? a) Yes. b) No.
29	Does the operator and participants of a wholesale payment system or a messaging network leverage existing cybersecurity working groups to incorporate fraud-related elements of the strategy to reduce the risk of wholesale payments fraud related to endpoint security into their plans? a) Yes. b) No.

Cyber deterrence

Q. No	Question and multiple-choice answers
30	Is there a cybercrime regulation in place in your jurisdiction, which sets out the different types of cybercrime, the role and responsibilities of law enforcement authorities, the processes for prosecuting cyber criminals and the punishment to be meted out to such criminals? a) Yes. b) No.
31	What are the arrangements for dealing with cyber incidents with the help of law enforcement authorities? a) Law enforcement authorities have specialized cyber units and are responsible for combatting, preventing, disrupting, investigating, and prosecuting cybercrime and cyber criminals. The law enforcement authorities have a close working relationship with the central bank and financial entities. b) Law enforcement authorities have specialized cyber units and are responsible for combatting, preventing, disrupting, investigating, and prosecuting cybercrime and cyber criminals. The law enforcement authorities do NOT have a close working relationship with the central bank and financial entities. c) There are no specialized cyber-related law enforcement arrangements in place.
32	What arrangements are there between law enforcement authorities, the central bank, and financial entities to ensure prosecution of cyber criminals? a) There is clear guidance and processes between law enforcement authorities, the central bank, and financial entities on how to report cybercrime, retain digital evidence, and to transfer this evidence to aid prosecution of cyber criminals. b) There is clear guidance and processes between law enforcement authorities and financial entities on how to report cybercrime, retain digital evidence, and to transfer this evidence to aid prosecution of cyber criminals. The central bank is not involved in this process. c) There is no clear guidance and processes between law enforcement authorities, the central bank, and financial entities on how to report cybercrime, retain digital evidence, and to transfer this evidence to aid prosecution of cyber criminals.
33	What coordination is there in place with CERT and law enforcement authorities? a) The central bank runs the financial sector CERT (FinCERT) and coordinates with law enforcement agencies effectively. b) The FinCERT is a separate entity not run by the central bank. The central bank and CERT/FinCERT coordinate their activities well. c) The central bank coordinates effectively with the CERT. There is no FinCERT in the country. d) The central bank rarely gets in touch with the CERT. Activities are not well coordinated. e) There is no CERT in the country.

Financial stability analysis

Q. No	Question and multiple-choice answers
34	Have you developed a "cyber map" that identifies the main technologies, services, and connections between financial sector institutions, service providers, and in-house or third-party systems? a) Yes, we have developed a cyber map of our financial sector and use it as a reference for supervisors to identify key vulnerabilities and allocate resources. b) Not yet; however, we have collected the relevant information required to produce a cyber map, which we intend to complete in the next 12 months. c) No, and we do not have the requisite information available to produce a cyber map.

35	Do you conduct quantitative analysis of cyber risk in your jurisdiction? a) Yes, we collect data on frequency and loss from cyberattacks and have a methodology to quantify potential future losses. b) No, we do not collect the relevant data and do not have a methodology to quantify cyber risk and potential future losses stemming from cyberattacks.
36	Does your stress test program include cyber risk? a) Yes. b) No.
37	What proportion of your financial sector has migrated part of or all of their functions to cloud service providers? a) Most financial institutions. b) Several financial institutions. c) The minority of financial institutions. d) This information is not available.

Continuous learning and capacity development

Q. No	Question and multiple-choice answers
38	What is the approach to strengthening cyber risk supervisory capacity? a) There is no formalized approach yet; decisions are made as needs arise. b) There is a general capacity development plan that is implicitly applicable to cyber risk supervision as well. c) There is a capacity development plan that is specific to cyber risk supervision.
39	What approaches are used to raise cybersecurity awareness in the financial sector and the public at large? **(Select all that apply)** a) Workshops with key stakeholders. b) Participating in, or encouraging public-private partnerships. c) Interviews, speeches, and publications. d) Co-operation with academia.
40	Which cybersecurity training options are available for supervisors? **(Select all that apply)** a) Free webinars and online courses. b) Certification training and exams (for example, CISA, CISSP, and so on) subsidized by the authority. c) Academic programs (for example, undergraduate, graduate, or postgraduate) subsidized by the authority.
41	Is an academic degree in IT required to become a cyber risk supervisor? a) Yes. b) No.
42	Do you require cyber risk supervisors to obtain and maintain relevant professional certifications? a) No. b) Yes, for senior supervisors. c) Yes, for all.
43	Please provide any additional comments you may have.

ANNEX 2. Instructions to Fill Out the Survey

Annex Box 2.1. Instructions to Respondents

What is the deadline for completion/return?

The completed questionnaire should be returned to the IMF within four weeks of receipt.

Who should complete the questionnaire?

The questionnaire should be completed by competent parties with appropriate knowledge and experience, specifically in the subject matter of cyber risk supervision and oversight.

How should the central bank or supervisory agency answer if more than one answer applies?

In case there is more than one answer that applies, select all that apply, and you may provide an explanatory note at the end of the survey in the text box if necessary.

Can any questions be left blank if the central bank or supervisory agency is uncertain of the current position for the jurisdiction?

No. All questions must be answered to the central bank or supervisory agency's best ability.

Will the central bank or supervisory agency need to provide documentation and information that supports the answer selected?

No. This questionnaire is not an assessment of the jurisdiction's cyber capabilities or maturity. The questionnaire aims to collect data on key elements around cybersecurity of the financial sector to further aid the IMF in developing tools to build capacity globally.

Source: IMF staff.

ANNEX 3. Cybersecurity Preparedness Index: Detailed Methodology

Cybersecurity Preparedness Index–Indicators and Methodology

The Cybersecurity Preparedness Index is constructed based on 15 survey questions most reflective of a jurisdiction's cybersecurity preparedness. Based on expert judgment, each question is assigned a score between 5 (best preparedness) and 0 (worst preparedness). The Cybersecurity Preparedness Index is the weighted average of the individual scores, where 5 out of the 15 questions are considered baseline requirements and are given a weight of 10 percent and the remaining 10 questions are assigned a weight of 5 percent. Annex Table 3.1 provides an overview of the selected questions, assigned points, and weights.

Annex Table 3.1. Construction of the Cybersecurity Preparedness Index

Relevant Question	Weightage (%)	Max Score	Scoring Formula	Marks
2. Does your jurisdiction have a national cyber strategy, which includes the financial sector?	5	5	No.	0
			No, we do not have a national cyber strategy, although there are ongoing discussions on whether we should develop such a strategy.	0
			No, but the government is developing a strategy that is expected to be finalized in the next 12 months (without active involvement of the central bank/supervisors).	1
			No, but we, as the central bank or supervisory agency, are currently working on a government-driven national cyber strategy, that is expected to be endorsed in the next 12 months.	2
			Yes, we have a national cyber strategy, which includes the financial sector.	5
3. Does your central bank or supervisory agency have a cyber strategy for the financial sector?	5	5	No.	0
			No, but we are currently developing one and expect to publish it within the next 12 months.	1
			Yes, however, it is separate and not connected to the national cyber strategy.	3
			Yes, and it is integrated into the national cyber strategy.	5
8. Does your jurisdiction have a dedicated and published cybersecurity or technology risk management regulation for the financial sector?	10	5	No.	0
			No, we do not have a dedicated cybersecurity or technology risk management regulation but include this risk area as part of our operational or risk management regulation.	2
			No, but we are currently developing a cybersecurity or technology risk management regulation, which will be published in 12 months.	3
			Yes, we have a dedicated cybersecurity or technology risk management regulation, which has been published.	5

Relevant Question	Weightage (%)	Max Score	Scoring Formula	Marks
10. Does your jurisdiction have a dedicated and published data privacy regulation?	5	5	No.	0
			No, but we are currently developing one, which will be published in 12 months.	2
			Yes.	5
11. How is the supervisory architecture organized within your jurisdiction?	10	5	We do not take support from the IT department, and ICT/cyber risk work is handled by generalists in an ad hoc manner.	1
			We do not have a specialized Cyber Risk Unit as of now, but we are planning to have one soon.	2
			We leverage the skill set of our IT department to conduct ICT/cyber examinations, but these are coordinated by the Supervision Department.	3
			We have a specialized Cyber Risk Unit outside the Supervision Department.	4
			We have a specialized Cyber Risk Unit as part of the Supervision Department.	5
13. What are the methods deployed for on-site supervision of cyber risk?	10	5	We do not conduct on-site examinations. We do not have the legal powers to mandate external audits or forensic investigations.	0
			We require an external audit of cyber preparedness of banks/FMIs on a yearly basis.	1
			We have limited capacity to conduct on-site examinations.	2
			We conduct predominantly thematic reviews. Full scope examinations are rare, but we do limited scope examinations at times. We have legal powers to mandate external audits or forensic investigations.	3
			We conduct on-site supervision (full scope or limited scope examination). Thematic reviews are generally not used, but we have legal powers to mandate external audits or forensic investigations.	4
			We have a full range of approaches (full scope examination, limited scope examination, short visits, and thematic reviews) as well as the legal powers to mandate external audits and forensic investigations.	5
14. What are the arrangements for off-site supervision of cyber risk?	5	5	At this juncture, we do not have any plan to set up an off-site function for ICT/cyber.	0
			We do not have a dedicated off-site function, but we have the capability to collect ad hoc information at a short notice.	1
			We have just established an off-site function and currently collect very limited information. We plan to strengthen the off-site function significantly in the coming year.	2
			We have a separate off-site function which collects data, which we analyze regularly.	4
			We collect a full range of off-site information that pertains to ICT/cyber. We carry out analysis of such data with a focus to identify material risks faced by the individual entity as well as the system as a whole, and we provide key inputs to the on-site team.	5

Relevant Question	Weightage (%)	Max Score	Scoring Formula	Marks
15. Do you have powers to conduct an on-site inspection of third-party providers, if necessary?	5	5	Unclear.	0
			No.	0
			Yes.	5
19. How do you deal with cybersecurity incidents occurring at supervised institutions? (Select all that apply.)	5	5	We have not established the process yet.	0
			On-site direction and control of response and recovery activities.	2
			On-site involvement in response and recovery without taking control (that is, advisory role).	3
			Off-site monitoring of the response and recovery activities of the institution.	4
			Analyzing mandatory reporting of cyber incidents.	5
25. Do you have a cyber incident reporting regime in place?	10	5	No.	0
			No, we don't have a dedicated and specific cyber incident reporting regime in place, but financial institutions are required to report incidents as part of their operational risk requirements.	2
			Yes, we have a dedicated cyber incident reporting regime and financial institutions are required to report incidents by law or regulation.	5
20. What is your approach to cybersecurity testing and exercises (such as penetration tests, red teaming, and effectiveness of cyber incident response and crisis management exercises)?	10	5	There is a mandatory cybersecurity testing regime that is actively managed by the authorities.	5
			Tests and exercises are required, and there is further guidance (for example, on scope, coverage, periodicity, or methods).	4
			Tests and exercises are required, but there is no further guidance.	3
			Tests and exercises are encouraged but currently not required.	1
32. What are the arrangements for dealing with cyber incidents with the help of law enforcement authorities?	5	5	There are no specialized cyber-related law enforcement arrangements in place.	0
			Law enforcement authorities have specialized cyber units and are responsible for combating, preventing, disrupting, investigating, and prosecuting cybercrime and cybercriminals. The law enforcement authorities do not have a close working relationship with the central bank and financial entities.	3
			Law enforcement authorities have specialized cyber units and are responsible for combating, preventing, disrupting, investigating, and prosecuting cybercrime and cybercriminals. The law enforcement authorities have a close working relationship with the central bank and financial entities.	5
39. What is the approach to strengthening cyber risk supervisory capacity?	5	5	There is a capacity development plan that is specific to cyber risk supervision.	5
			There is a general capacity development plan that is implicitly applicable to cyber risk supervision as well.	3
			There is no formalized approach yet; decisions are made as needs arise.	0

Relevant Question	Weightage (%)	Max Score	Scoring Formula	Marks
40. What approaches are used to raise cybersecurity awareness in the financial sector and the public at large? (Select all that apply.)	5	5	Cooperation with academia.	5
			Interviews, speeches, and publications.	
			Participating in or encouraging public–private partnerships.	
			Workshops with key stakeholders.	
			All 4	
			3 out of 4	4
			2 out of 4	3
			1 out of 4	2
			None	1
42. Do you require cyber risk supervisors to obtain and maintain relevant professional certifications?	5	5	No.	0
			Yes, for all.	5
			Yes, for senior supervisors.	4
	100	75		

Source: IMF staff.

REFERENCES

Basel Committee on Banking Supervision (BCBS). 2021a. "Principles for Operational Resilience." March. https://www.bis.org/bcbs/publ/d516.pdf

Basel Committee on Banking Supervision (BCBS). 2021b. "Revised Principles for the Sound Management of Operational Risk." March. https://www.bis.org/bcbs/publ/d515.pdf

Council of Europe (CoE), Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), and others. 2021. *Guide to Developing a National Cybersecurity Strategy 2nd Edition—Strategic Engagement in Cybersecurity*. Creative Commons Attribution-NonCommercial 3.0 IGO (CC BY-NC 3.0 IGO). https://ncsguide.org/the-guide/

CPMI-IOSCO. 2016. "Guidance on Cyber Resilience for Financial Market Infrastructures." June. https://www.bis.org/cpmi/publ/d146.pdf

CPMI-IOSCO. 2019. "Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security: A Toolkit." https://www.bis.org/cpmi/publ/d188.pdf

ENISA. 2023. "A Governance Framework for National Cybersecurity Strategies." February. https://www.enisa.europa.eu/sites/default/files/publications/A%20Governance%20Framework%20National%20Cybersecurity%20%20Strategies.pdf

European Banking Authority (EBA). 2019. "Final Report: EBA Guidelines on ICT and Security Risk Management." https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

Financial Stability Board (FSB). 2019. "Third-Party Dependencies in Cloud Services—Considerations on Financial Stability Implications." https://www.fsb.org/wp-content/uploads/P091219-2.pdf

Financial Stability Board (FSB). 2020. "Effective Practices for Cyber Incident Response and Recovery." Basel. https://www.fsb.org/uploads/P191020-1.pdf

Financial Stability Board (FSB). 2023a. "FSB Publishes Toolkit for Enhancing Third-Party Risk Management and Oversight." https://www.fsb.org/2023/12/fsb-publishes-toolkit-for-enhancing-third-party-risk-management-and-oversight/

Financial Stability Board (FSB). 2023b. "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting." https://www.fsb.org/wp-content/uploads/P130423-1.pdf

Forscey, David, Jon Bateman, Nick Beecroft, and Beau Woods. 2022. "Systemic Cyber Risk: A Primer." CEIP Paper, March 7. https://carnegieendowment.org/research/2022/03/systemic-cyber-risk-a-primer?lang=en

Group of Seven (G7). 2017a. "G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector." https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2017-G7-fundamental-elements-for-effective-assessment-of-cybersecurity-in-the-financial-sector.en.pdf

Group of Seven (G7). 2017b. "G7 Fundamental Elements of Cybersecurity for the Financial Sector." https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

Group of Seven (G7). 2018. "G7 Fundamental Elements for Threat-LED Penetration Testing." https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2018-G7-fundamental-elements-for-threat-led-penetration-testing.en.pdf

Group of Seven (G7). 2020. "G7 Fundamental Elements of Cyber Exercise Programs." https://www.ecb.europa.eu/paym/pol/shared/pdf/November_2020-G7-fundamental-elements-of-cyber-exercise-programmes.en.pdf

Group of Seven (G7). 2022a. "G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector." https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2022-G7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector.en.pdf

Group of Seven (G7). 2022b. "G7 Fundamental Elements of Ransomware Resilience for the Financial Sector." https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2022-G7-Fundamental-elements-of-ransomware-resilience-for-the-financial-sector.en.pdf

International Association of Insurance Supervisors (IAIS). 2016. "Issues Paper on Cyber Risk to the Insurance Sector." August. https://www.iaisweb.org/uploads/2022/01/160812-Issues-Paper-on-Cyber-Risk-to-the-Insurance-Sector_final.pdf

International Association of Insurance Supervisors (IAIS). 2023. "Issues Paper on Insurance Sector Operational Resilience." May. https://www.iaisweb.org/uploads/2023/05/Issues-Paper-on-Insurance-Sector-Operational-Resilience.pdf

International Monetary Fund (IMF). 2024. "Cyber Risk: A Growing Concern for Macro-Financial Stability." In *Global Financial Stability Report*. Washington, DC, April. https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024

PUBLICATIONS

Strengthening Cybersecurity: Lessons from the Cybersecurity Survey

TNM/2025/06

ISBN 9798400296864