INTERNATIONAL MONETARY FUND

Monetary and Capital Markets Department

Cybersecurity Risk Supervision

Christopher Wilson, Tamas Gaidosch, Frank Adelmann, and Anastasiia Morozova

No. 19/15

Monetary and Capital Markets Department

Cybersecurity Risk Supervision

Christopher Wilson, Tamas Gaidosch, Frank Adelmann, and Anastasiia Morozova

INTERNATIONAL MONETARY FUND

Cataloging-in-Publication Data
IMF Library

Names: Wilson, Christopher (Christopher Lindsay), author. | Gaidosch, Tamas, author. | Adelmann, Frank, author. | Morozova, Anastasiia, author. | International Monetary Fund. Monetary and Capital Markets Department, issuing body. | International Monetary Fund, publisher.
Title: Cybersecurity risk supervision / Christopher Wilson, Tamas Gaidosch, Frank Adelmann, and Anastasiia Morozova.
Other titles: International Monetary Fund. Monetary and Capital Markets Department (Series).
Description: Washington, DC : International Monetary Fund, 2019. | At head of title: Monetary and Capital Markets Department. | Departmental paper series. | Includes bibliographical references.
Identifiers: ISBN 9781513507545 (paper)
Subjects: LCSH: Financial institutions—Risk management. | Financial institutions—Computer networks—Security measures. | Hacking—Prevention.
Classification: LCC HG173.W55 2019

Publication orders may be placed online, by fax, or through the mail:
International Monetary Fund, Publication Services
P.O. Box 92780, Washington, DC 20090, U.S.A.
Tel. (202) 623-7430 Fax: (202) 623-7201
E-mail: publications@imf.org
www.imfbookstore.org
www.elibrary.imf.org

Contents

Executive Summary

This paper highlights the emerging supervisory practices that contribute to effective cybersecurity risk supervision, with an emphasis on how these practices can be adopted by those agencies that are at an early stage of developing a supervisory approach to strengthen cyber resilience. Financial sector supervisory authorities the world over are working to establish and implement a framework for cyber risk supervision. Cyber risk often stems from malicious intent, and a successful cyber attack—unlike most other sources of risk—can shut down a supervised firm immediately and lead to systemwide disruptions and failures. The probability of attack has increased as financial systems have become more reliant on information and communication technologies and as threats have continued to evolve.

The first line of defense against cybersecurity risk rests with financial institutions' own risk management, but supervisory authorities also play a crucial role in ensuring resilience of both firms and the system. Information gathering and analysis, including through established relationships with other national agencies and with supervisors in other jurisdictions, will allow supervisors to develop an understanding of the evolving nature of attacks ("threat landscape"). Developing a "cyber map" of key elements of the financial sector (for example, payment systems, exchanges, financial market infrastructures, and financial institutions), including key technology systems in use by each supervised firm, will give supervisors a systemwide view against which to assess the threat landscape and anchor the supervisory program.

Regulatory requirements ensuring that good cybersecurity risk management practices are in place are critical. Supervisory expectations (expressed in regulations, standards, guidance, etc.) should build on existing and widely embraced technical standards and should be developed in consultation with the financial sector. Regulation should be complemented by sound and consistent supervisory practices, testing mechanisms that will better inform response planning, and timely reporting and information-sharing arrangements. A continuous improvement process for regulatory frameworks and supervisory practices is needed.

Supervisory authorities should build on risk assessments undertaken by supervised firms. By understanding a firms' information assets; their relative importance in the financial sector; protection requirements in terms of confidentiality, integrity, availability; and the maturity of their cybersecurity management, supervisory authorities can better implement a risk-based approach to supervision. Both offsite and onsite supervisory review processes should include cybersecurity risk. Regulation and supervision of key third-party service providers—in particular, where there is a concentration of services in a few providers—is another important element. Boards of directors and senior management should also be expected to take responsibility for cyber resilience and broader business technology risks.

Security testing exercises with focus on detection, response, and recovery are core elements of building resilience. Even highly sophisticated cyber defenses can expect to be breached, hence effective processes are needed to detect intrusion, stop the attack, and facilitate quick recovery. Cyber attack simulation exercises should be conducted at the firm level to help inform continuous improvement in resilience. Sector-wide tests involving public and private participants will complement firm-level exercises and deepen the understanding of response and recovery protocols as well as information sharing. Crisis management planning by supervisors and various agencies tasked with oversight of the financial system is needed to complement exercises by the private sector.

Strong information sharing and reporting practices underpin the supervisor's ability to understand and oversee cybersecurity risk management. Well-defined and enforced incident reporting by firms will provide supervisors with timely and critical information on the threat landscape, and resilience and responsiveness of firms. Supervisors can facilitate sharing information between firms to enhance collective resilience and can coordinate with other public sector agencies if necessary.

The task of combating cybersecurity risk can appear daunting, especially for supervisory authorities facing resource constraints, but some key actions must be taken by all. Recent experience has demonstrated that no corner of the global financial system is immune to cyber attacks. All supervisory agencies, even those facing significant constraints, are called upon to quickly establish a framework for cybersecurity risk supervision. Experience from IMF technical assistance shows that this is indeed a challenge and that the dearth of specialist skills is one of the biggest challenges.[1] Notwithstanding these, all supervisors can take action to build information-gathering and sharing systems, improve basic security practices ("cyber hygiene"[2]), and identify and deploy resources toward key assets and carry out basic cyber exercises.

[1]An IMF survey of 40 developing jurisdictions revealed that 92.5 percent face skills shortages in cybersecurity regulation and supervision. Anecdotal evidence points to a similar situation in advanced economies.

[2]Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security.

Glossary

BCBS	Basel Committee for Banking Supervision
CPMI	Committee on Payments and Market Infrastructures
EU	European Union
FFIEC	Federal Financial Institutions Examination Council
G7	Group of 7 Countries (Canada, France, United States, United Kingdom, Germany, Japan, and Italy)
ICT	information and communication technology
IOSCO	International Organization for Securities Commisions
ISO	International Organization for Standards
RTO	recovery time objective
RPO	recovery point objective
SSB	standards-setting body

Overview

Strengthening cybersecurity[1] in the financial sector is a priority for financial stability. The financial sector is a high-profile target for cyber threat actors, and cyber risks are a danger to the stability of national and global financial systems owing to potential cross-border spillovers. The financial sector is highly, and increasingly, dependent on information and communication technologies (ICT). A cyber attack can disrupt the provision of critical functions, threaten liquidity, and destabilize the integrity of the financial system.

Although efforts to encourage better cyber resilience of the financial sector are progressing globally, practice is uneven. Technical standards providing guidance to risk managers have been developed in the private sector, are well-advanced, and are in use around the world. Global standards-setting bodies have published guidance with work ongoing demonstrating leading-edge frameworks and approaches (Basel Committee on Banking Supervision 2018). At the national level, jurisdictions are updating regulatory requirements and developing supervisory practices to promote cyber resilience. Progress, however, is uneven, particularly for lower-income countries and lower-capacity supervisors, which face a number of challenges developing an effective regulatory and supervisory framework for cyber risk supervision.

[1]Cybersecurity, cybersecurity risk, and cyber resilience are widely but imprecisely used terms. In this paper we use the Financial Stability Board's Cyber Lexicon definition of cybersecurity ("Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved"), which is broad and considers cyber incidents irrespective of their cause, and where "cyber" relates to the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Thus, for all practical purposes, the term cybersecurity is the same as information security that has been broadly used for some time. Similarly, cyber resilience can be considered a new term referring to the existing concept of business continuity management but with a focus on cyber threats.

This paper highlights emerging supervisory approaches with the intention of promoting good practices. The paper draws on technical assistance work conducted by the IMF and on multilateral outreach with constituents and standards-setting bodies. Importantly, the paper identifies priorities for agencies in the process of establishing a regulatory and supervisory framework for supervision of cybersecurity risk, with a view to implementation that can overcome challenges typically faced by lower-income and lower-capacity supervisory agencies.

CHAPTER

1 The Nature of the Risk

The cyber threat landscape is highly dynamic and threat actors continue to evolve. Attacks against ICT systems have the potential to endanger financial stability.

High-profile incidents demonstrate the potential impact of cyber attacks.[1] According to a recent report, cyber crime costs businesses close to US$600 billion annually, up from US$445 billion in 2014 (McAfee and Center for Strategic & International Studies 2018). A 2017 survey estimated that a typical financial institution faces an average of 85 targeted cyber attacks every year, a third of which are successful (Accenture 2017). An IMF staff modeling exercise published in 2018 estimates that annual losses to financial institutions from cyber attacks could reach several hundred billion dollars a year in an extreme scenario, eroding bank profits and potentially threatening financial stability (Bouveret 2018). As malware is easily available in the dark net, cyber attacks against supervised firms are becoming easier, more common, and considerably more sophisticated. At the same time the impact of cyber attacks is increasing due to the growing interconnectedness and complexity of ICT systems in the financial sector and beyond—most notably in the telecommunication sector, a key dependency of most financial services. Although estimates of the number and costs of cyber crime vary, they all follow an upward trajectory.

The cyber threat landscape is highly dynamic and rapidly changing. The nature of cyber attacks and threat actors continue to evolve. For example, the nature of attacks has changed from predominantly destructive malware in 2015–16 to mainly phishing attacks in 2018. Equally, the modus operandi of threat actors is changing as the proliferation of cyber attack tools has lowered costs and made it easier for sophisticated methods to be used by a wide range

[1]Carnegie Endowment for International Peace published a timeline of cyber incidents involving financial institutions at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

of actors at low cost.[2] Access to increasingly sophisticated hacking tools has become widespread and cost-effective for cyber criminals. The extensive use of outsourcing by the financial sector creates an additional layer of complexity and, if not well managed, may increase overall risk. Given the inherent interconnectedness of financial sector participants, disruption to the payment, clearing, or settlement systems or theft of confidential information can result in widespread spillovers and threaten financial stability.

Cybersecurity risk has unique characteristics. A distinguishing characteristic of sophisticated cyber attacks is the often-experienced persistent nature of a campaign conducted by motivated threat actors (also called advanced persistent threats). In this scenario, hackers can apply themselves to a target over a long period of time, often lurking inside a target's system for months, learning the system's features and defenses before finalizing the attack. In comparison to financial risks and other physical risks, there is a much broader range of entry points through which the financial sector can be compromised. Another unique feature of cybersecurity risk is the ability of some cyber attacks to render some risk management and business continuity arrangements ineffective. For example, real-time data duplication to a remote site is a well-known arrangement for improving business continuity; however, data corrupted by cyber criminals will also be duplicated to the remote site in real time, which can cancel the benefit of this mechanism. And lastly, cyber attacks can be stealthy and propagate rapidly within a network of systems (Committee on Payments and Market Infrastructures [CPMI] and Board of the International Organization of Securities Commissions [IOSCO] 2016). For example, many malware strains search and infect vulnerable systems automatically and spread silently on an exponential scale before activating their payload. Attackers can be well-resourced and organized using very advanced attack methods and may have destruction rather than profit motives, which further complicates defense. Cyber attacks are regarded as a national defense issue in some circumstances, bringing the financial supervisory authorities into contact with national security considerations in a way that is normally absent from their activities.

Whereas certain dimensions of cybersecurity exhibit unique risk characteristics, regulations should align closely with broader ICT and operational risk management practices. Experience suggests that a range of approaches to cyber resilience exist (Basel Committee on Banking Supervision 2018). In those jurisdictions covered by the BCBC range of practice paper, broader information technology and operational risk management practices are quite mature and are used to address cybersecurity risk and supervise cyber resil-

[2]We have also seen some threat actors (for example, typical categories of threats actors include national states, proxy organizations, cyber criminals, hacktivists, and insiders) wholesaling their services and adopting models such as outsourcing and vertical integration (for example, organized crime syndicates).

ience. Additionally, most supervisors leverage previously developed national or international standards—principally the National Institute of Standards and Technology's Cybersecurity Framework,[3] International Organization for Standardization (ISO) standards 27000 series, and CPMI/IOSCO guidance for cyber resilience of financial market infrastructures (CPMI/IOSCO 2016) (see the section titled "Regulation").

Several papers discuss key transmission channels through which cybersecurity risk can impact financial stability.

- The Office of Financial Research of the US Department of the Treasury described five steps through which an attempt to disrupt ICT could create financial instability: (1) a cyber incident is attempted, (2) defenses fail, (3) the incident creates a shock, (4) risk spreads through transmission channels, and (5) financial stability is affected.
- According to the Office of Financial Research's Financial Stability reports from 2016 and 2017, the key transmission channels through which cybersecurity incidents can threaten financial stability are the lack of substitutability for a key service or utility, the loss of customers or market participants, and the loss of data integrity as key transmission (Office of Financial Research 2016, 2017).
- The International Institute for Finance published four key scenarios that could harm financial stability: (1) attack on payment systems, (2) integrity of data, (3) failure of wider infrastructure, and (4) loss of confidence (Institute of International Finance 2017).
- Acknowledging that operational disruptions can impact financial stability, the Bank of England and the UK Financial Conduct Authority published a discussion paper to generate debate about the expectations regulators and the wider public might have of the operational resilience of financial services institutions (Bank of England 2018).

[3]Several other national standard setters (such as German Federal Office for Information Security or French National Cybersecurity Agency) are also widely recognized in this space.

CHAPTER

2 Achieving Cyber Resilience

The goal of cybersecurity risk supervision should be to influence, incentivize, and shape firms' cybersecurity capabilities. Supervision activities to build resilience should include the following: identify the threat landscape; map the cyber and financial network; create coherent regulation; conduct supervisory assessment; establish formal information sharing and reporting mechanisms; provide adequate response and recovery; and ensure preparedness of supervisory agencies.

The goal of cybersecurity risk supervision should be to influence, incentivize, and shape firms' cybersecurity capabilities (see Figure 1). Although cybersecurity risks will never be fully mitigated, the regulatory framework and supervision activities need to adequately incentivize supervised firms and relevant third parties (for example, technology providers) to implement robust risk management techniques. Firms might not naturally internalize spillovers and externalities from their own failure; therefore, the supervisor has a crucial systemwide role to take account of the systemwide aspects. The task of combating cybersecurity risk can appear daunting, especially for supervisory authorities facing resource constraints, but given the importance and pervasiveness of the risk, cybersecurity risk management must be fully integrated into supervision of all firms. To put it another way, supervisory authorities cannot fully understand and address the risk profile of a supervised firm or financial stability without also understanding and addressing cybersecurity risk. Building skills and supervisory resources is a key challenge for all supervisory authorities, but one that must be a priority to address.

As cyber attacks do not know borders, information-sharing and reporting are essential elements to combat cyber threats. Although there are different views on the format and platforms that should be used to share threat intelligence, cooperation among authorities and supervised firms should be strengthened to enhance cyber resilience for the interconnected global financial system. Data protection requirements should be considered when setting

Figure 1. Supervision to Build Resilience

Source: IMF staff.

up information-sharing platforms. However, these should not be used as excuse for not sharing information at all. Sufficiently detailed anonymized data shared on appropriate platforms help to properly and timely react to cyber threats.

Identifying the Threat Landscape

Supervisors should use information gathering and analysis to understand the evolving nature of attacks. Supervisors need to develop relationships with other national agencies[1] dealing with cyber attacks, for example, national computer emergency response teams, cyber crime units in law enforcement, and supervisors in other jurisdictions. Further, supervisors should gather information from industry sources. Cyber threat information can include technical indicators (such as malicious internet protocol addresses, domains, indicators of compromise, etc.); adversary tactics, techniques, and procedures; best practices; security tool configurations; threat analysis; and cyber incident details. The goal of the information gathering and analysis is to help build a threat profile for each individual supervised firm, and in their combination a threat profile for the complete financial sector.

[1]Examples for such agencies are the Federal Office for Information Security in Germany, the Agence Nationale de le Securite des Systems d'Information in France, the Cybersecurity Agency in Singapore, or the Israel National Cyber Directorate. In addition, several national and international bodies have implemented permanent computer emergency response teams to reduce the risk of systemic cybersecurity breaches and address communications challenges on a national/international level, such as the US-CERT or CERT-EU.

Incident reporting by supervised firms is a key component of understanding the threat landscape. Well-designed incident reporting frameworks are needed to help gather data on trends in the development of the cyber threat landscape. Arrangements for information exchange and reporting can help lay the foundation for data collection. Convergence in taxonomies for cyber incidents and templates for the incident reporting is underway, making the data more comparable. The Financial Stability Board published a "Cyber Lexicon" in November 2018, comprising a set of approximately 50 core terms related to cybersecurity and cyber resilience in the financial sector (Financial Stability Board 2018). The Cyber Lexicon can help support cross-sector common understanding of relevant cybersecurity and cyber resilience terminology and lay the foundation for effective information sharing (see also the section title "Information Sharing and Reporting").

Mapping the Cyber and Financial System

A full picture of supervised firms and their ICT systems will underpin a supervisor's understanding of vulnerabilities in the financial system. There are two distinct steps to this process: (1) firm level and (2) sector wide. An in-depth understanding of a firm's ICT systems is the first step in this process. This step should build on supervisors' general knowledge of their supervised firms' business models, management of ICT risks, and importance for the financial sector. The second step is to consolidate firm-specific financial and technical connections to form a systemwide view—a financial sector network map that combines financial connections between systemic firms and their respective ICT connections (see Figure 2 and Annex 2). Added to this should be the identification of key technology systems in use by each supervised firm (whether they are in-house or delivered by third parties), as the usage of similar ICT systems can make supervised firms vulnerable to the same cyber attack techniques. Knowledge of both financial and technical connections will help the supervisor to conduct firm-level supervisory risk assessments (for example, operational risk assessments, including ICT risk).

Mapping financial and technology connections across the sector will help identify potential systemic risks from interconnectedness and concentrations in third-party service providers. Assessing interconnectedness of the financial system network is essential for understanding how a shock to one supervised firm/utility/service provider can spread to others, potentially leading to a cascade of liquidity shortage, write-downs, and defaults. Identification of key nodes in the financial system—for example, the payment and settlement system, financial institutions that carry out key services such as clearing and the technology systems underpinning them—should be done to understand cyber risk on a systemwide basis. The mapping of the financial sector net-

work can be used to estimate the impact of a cyber attack on any of the nodes. The cyber map will also assist in identifying potential concentration risks in third-party service providers.

A diverse range of approaches to cyber mapping can be used by supervisors depending upon the size, scale, and complexity of the system. For smaller, less-complex financial systems, cyber mapping could be a relatively straightforward exercise consisting of identification of key technology systems used by individual financial institutions as well as a list of material third-party service providers consolidated to form a systemwide view. As it can be seen in Figure 2, the analysis would help supervisors identify the financial and network connections between systemic institutions in the system (for example, banks, exchanges, and payment systems, etc.). For example, a supervisor may follow a relatively basic process:

- Step 1. Identify main systemic institutions in the financial sector and extent of financial flows.
- Step 2. Survey systemic institutions (identified in Step 1) to detail the use of primary ICT including service providers.
- Step 3. Aggregate firm-specific data to form a sector-wide view of the use of ICT by systemic institutions to identify potential concentrations of platforms, service providers, etc.

For more complex systems, a more elaborate approach to cyber mapping may be needed. An emerging approach to cyber mapping consists of combining financial sector interlinkages with network linkages.[2]

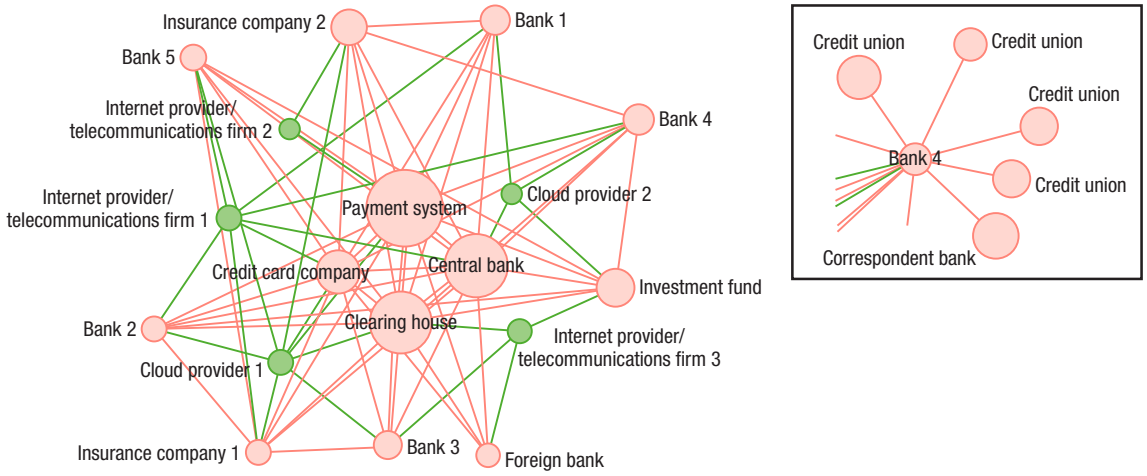
The mapping process may help identify dependencies of the financial sector on critical infrastructure. By mapping the cyber and financial network, supervisors will identify dependencies on critical infrastructure (for example, telecommunications, power, etc.). Supervisors should play a role in the national effort to identify critical infrastructure, which will include the payment system and systemically important financial institutions. Connecting to the national process for protection of critical infrastructure will provide supervisors with additional resources and support to address potential vulnerabilities.

Regulation

A strong regulatory and supervisory framework should allow supervisors to substantially improve the financial sector's resilience to cyber attack. Whether the regulatory framework is based on principles or rules, the framework must grant supervisors sufficient authority to address cybersecurity risk and allow

[2]Annex 2 describes one approach to assess the interconnectedness of the financial system network.

Figure 2. An Example of a Mapping Exercise



Source: IMF staff.
Note: FIs (supervised entities) are in pink; third-party technology providers (cloud service providers and internet providers) are in green. The size of the circle on the diagram is proportional to the degree of centrality, the measure of interconnectedness, and the importance of a node to the network. The stylized scheme illustrates a network in which important and central nodes, for example, a payment system, can be dependent on a single internet provider, making a technology firm a crucial piece of the system and revealing potential vulnerabilities. The inset shows that, while a node may be smaller than others, it may be a gateway to small institutions or correspondent relationships that are crucial to this particular sector.

supervisors to be sufficiently adaptive to the dynamics of the risk. Incident reporting should be robust and should inform the continuous improvement of resilience. Cybersecurity risk should be incorporated into offsite and onsite processes, and into the overall supervisory evaluation of a firm. Understanding the risk of reliance on third-party service providers should be a key priority for firms and regulators.

A combination of broad principles, outcome-focused rules (that provide detail on the implementation of principles), and baseline expectations that set out minimum requirements will form the basis for a robust framework. Regulations should focus more on "what to achieve" and less on "how to achieve." For example, requirements and expectations should be abstracted of technology-specific details and should predominantly state cybersecurity control objectives rather than require specific procedures or systems. The use of control objectives to describe the targeted cybersecurity stance can make frameworks more robust (for example, to withstand future changes of threat vectors, threat actor capabilities, and technologies). Although all firms face cybersecurity risk, smaller and lower-capacity firms should focus on strengthening cyber hygiene, whereas the largest and most globally connected firms and key system nodes should be subject to heightened standards. Authorities at a national and international level can work together to promote convergence regarding expectations of minimum standards and coordination and avoid unnecessary differences.[3]

[3]While regulatory consistency should be a key priority, differences in approaches will remain. Over the past two years, regulators around the world have issued a significant number of new cybersecurity rules. Financial

Regulations for cybersecurity should be flexible enough to allow supervisors to adjust quickly to the dynamic nature of the risks. Whereas supervisors may need to establish authority through clear prescription in laws and regulations, this should be balanced with sufficient flexibility to be able to react to and address the ever-evolving nature of the threat. A principles-based rather than a prescriptive approach allows industry to develop minimum levels of risk management with supervisory engagement clarifying expectations. Overly prescriptive regulatory frameworks may quickly result in outdated approaches or point-in-time compliance-based treatment of cybersecurity by supervised firms. Given the fluid nature of cyber risk, a point-in-time compliance-based treatment—based on outdated requirements—can lead to ineffective cybersecurity risk supervision.[4]

Regulation should be in place to make cybersecurity requirements enforceable and to allow the use of supervisory actions where needed. Cybersecurity regulation requirements, like in other areas of regulation, should be applicable to supervised firms in a manner proportionate to their risk. Requirements setting out the range of cybersecurity risk management controls ("control coverage") should apply to all supervised firms, but increased complexity and systemic importance should be reflected in how in-depth and sophisticated those controls become (referred to as "maturity") (see the section titled "Supervisory Assessment").

Cybersecurity regulation for supervised firms should be based on existing internationally accepted technical and regulatory standards and good practice. The existing technical and regulatory standards on cyber and information security are good starting points for any regulation or supervisory expectation relating to ICT or cyber risk. These technical standards, including the US National Institute of Standards and Technology Cybersecurity Framework, ISO standards (for example, the ISO 27000 series, ISO 22301, or ISO 31000), or Information Systems Audit and Control Association's Control Objectives for Information and Related Technology framework (Information Systems Audit and Control Association n.d.) are well-developed and widely in use. There are several viable, non-contradictive technical standards for cybersecurity risk management and firms may have substantially invested in

firms are spending significant resources juggling regulatory demands and implementing the new rules. In some instances, regulations are overlapping, duplicative, and conflicting. The result, in some circumstances, is to absorb time that would be better spent building stronger defenses.

[4]A discussion paper by Kashyap and Wetherilt (2018) furthermore suggests three principles that regulators can adopt when drafting regulation:

1. Insist that firms operate with the presumption that a successful attack is inevitable.
2. Insist that firms plan for prolonged and systemwide disruption, with particular attention to resourcing for response and recovery.
3. Aim for two-way dialogue between firms and supervisors about appropriate recovery times.3. Aim for two-way dialogue between firms and supervisors about appropriate recovery times.

one and therefore it can be counterproductive to require any specific standard. Expecting banks to generally follow existing technical standards, without enforcing a specific one, ensures the implementation of good practice while leveraging industry at the same time.

The Group of Seven countries (G7) Fundamental Elements of Cybersecurity for the Financial Sector could form the basis of regulation (see Box 1). This framework is succinct, easy to understand for nontechnical audiences, and easy to map to more detailed regulations and technical guidance.

Cybersecurity regulations should link to requirements for operational risk management, operational resilience, and business continuity generally.[5] Standards for operational risk management lay the foundation for more specific supervisory expectations in relation to cybersecurity (for example, Basel Committee for Banking Supervision [BCBS] Principles for the Sound Management of Operational Risk [BCBS 2011]). Common measures ensuring operational resilience and business continuity also mitigate cyber risk. For example, patch management (regular updates of existing software, including updates designed to address security flaws) is a classic ICT control area that also mitigates exposure to malware attacks, which is considered a cyber risk. Supervisors should weigh the advantages of the development and promulgation of a focused cybersecurity regulation versus a more comprehensive ICT risk management regulation. Either way, it is important to achieve consistency between cybersecurity and broader ICT risk management requirements.

The style and content of regulation will differ depending upon the jurisdiction, yet the maturity of risk management will be a key factor. Independent of the approach to regulation chosen,[6] providing a minimum standard for the sector will strengthen overall cyber resilience. Because of the high degree of interconnectedness, even small firms may have significant impact on the security and stability of the financial system. Building on the discussion of the high-level principles developed by the G7 (discussed in Box 1), the following topics should form the baseline of an effective regulation for all supervised firms:

[5]Operational resilience is a key element of business continuity management as defined by international standards. ISO 22301:2012, for example, defines business continuity management as "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities."

[6]BCBS identifies, describes, and compares the range of observed bank, regulatory, and supervisory cyber resilience practices across selected jurisdictions. See BCBS 2018.

Box 1. International Standard-Setting Efforts

The G7 has taken the lead in establishing a set of high-level principles for cybersecurity for the financial sector (Box Figure 1.1). The G7 Cyber Expert Group (CEG) comprising 23 financial authorities (finance ministries, central banks, and key regulators) across 8[1] jurisdictions has identified a set of fundamental elements of cybersecurity for the financial sector, reflecting best practices of G7 members.[2] The elements serve as the building blocks upon which public and private sector entities can design and implement their cybersecurity strategy and operating framework, informed by its approach to risk management and culture. Importantly, the elements are designed to be tailored and proportionate to the characteristics of each entity and the cyber risks it faces. In this way, the elements can be used by lower-income/lower-capacity countries as the foundations for a cyber defense architecture and a basis for regulations and supervision.

SSBs have identified tackling cyber risk supervision to be a high priority. SSBs, including the Basel Committee, CPMI-IOSCO, and IAIS—have built upon existing regulatory frameworks for the management of operational risks with supplemental guidance for cyber. The supplemental guidance focuses on aspects of risk management specific for cyber, such as information sharing, incident reporting etc. SSBs have established requirements for the management of operational risk that are high-level in nature and cover issues related to board and management oversight, security controls, legal and reputational risk management, business continuity and contingency planning, and managing outsourced activities as well as targeted guidance to complement more general requirements for operational risk management and specific topics such as business continuity and disaster recovery.

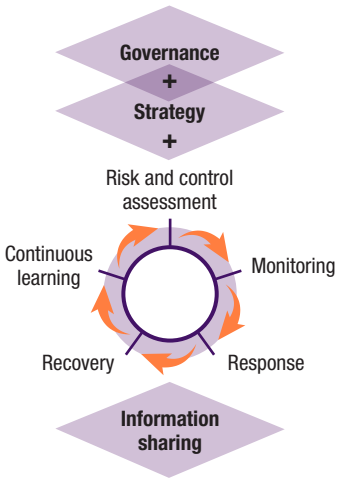
[1]The Group of Seven is an informal grouping of seven of the world's advanced economies comprising of: Canada, France, the United States, the United Kingdom, Germany, Japan, and Italy.

[2]The G7 Cyber Expert Group has published several guidelines to help promote cyber resilience. See for example: G7, G7 Fundamental Elements for Cybersecurity, October 2016, https://www.gov.uk/government/publications/g7-fundamental-elements-for-cyber-security.

- Assignment of cybersecurity risk management responsibilities to the board and senior management; documented cybersecurity program/policy and governance
- Designation of independent chief information security officer or equivalent
- ICT/cybersecurity awareness
- Identification of critical information assets, (cyber) threats, and vulnerabilities; assessment of control effectiveness
- Identity and access rights management
- Software development lifecycle

Box 1. International Standard-Setting Efforts *(continued)*

Box Figure 1.1. G7 High-Level Principles for Cybersecurity



Efforts at the international level laid the platform for work by national authorities, though implementation is mixed. A survey by the Financial Stability Board (FSB) of its membership showed that all members had used previously developed national or international guidance/standards when developing their own regulatory or supervisory schemes for the financial sector and many had complemented these standards with bespoke cyberguidance.[1] On the other hand, experience in non-FSB countries—particularly developing countries—suggests many supervisory authorities are yet to establish a bespoke regulatory framework for cybersecurity risk. Many jurisdictions are establishing national information technology/cybersecurity authorities, setting standards, coordinating reactions to cyber attacks, and supervising critical infrastructures in general, including banks and financial market infrastructures. Additional standards set by national security agencies are typically more granular and technical with the basic goal to protect the security of the society.

Source: Financial Stability Board, *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*, October 2017.
http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/.

[1]In 2017 the FSB published a stocktake of cyber risk regulations. The conclusions included the following: (1) all FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards; (2) about two-thirds of reported regulatory schemes take a targeted approach to cybersecurity and/or information technology risk and one-third address operational risk generally; (3) some elements commonly covered by regulatory schemes targeted to cybersecurity include risk assessment, regulatory reporting, role of the board, third-party interconnections, system access controls, incident recovery, testing, and training, (4) jurisdictions remain active in further developing their regulation and guidance. A total of 72 percent of jurisdictions reported plans to issue new regulations, guidance, or supervisory practices that address cybersecurity for the financial sector within the next year.

- Security event logging and monitoring; malware prevention; security reviews (such as vulnerability scans, penetration, or red team testing)
- Business and ICT continuity and operational resilience
- Vendor and outsourcing risks management
- Cyber incident reporting
- Number and know-how of cyber/information security professionals
- ICT governance and ICT strategy
- Physical and network security
- Independent information security reviews, assessment, and testing.

Regulation should emphasize the continuous improvement approach and the pivotal role of risk and control assessment in cybersecurity risk management. The continuous improvement cycle concept[7] is widely used in ICT and cybersecurity risk management systems, and it hinges on a realistic and comprehensive risk assessment. Regulation should promote minimum scope, timing, and follow-up requirements. However, it is recommended that regulation remains agnostic on the actual methodology, which should be assessed in the supervisory process.

Supervisory Assessment

Cybersecurity risk should be assessed as part of the supervisory review process.[8] Due to its large potential impact on a firm's viability, cyber risk is an important subcategory of operational risk. Cybersecurity risk assessments are often undertaken within the operational risk assessment as part of the ICT risk assessment. Cybersecurity risk is relevant to the assessment of a firm's governance, strategy, business model, and risks to capital. Cyber and ICT risks are typically considered material, as ICT systems form the backbone of almost all banking processes and distribution channels, support automated control environments on which core banking data is based, and are the key enablers of firms' strategy. The importance of ICT in strategic decisions is growing as technological innovation became a key source of competitive advantage.

Supervisory manuals based on the cybersecurity regulation need to be developed. Manuals set out concrete guidance on how to conduct a consistent assessment of a firm's ICT or cyber risk profile (inherent risk), and its ICT or cyber control maturity level. The ICT or cyber control maturity assessment should cover all relevant topics ensuring sufficient cyber hygiene for all supervised firms, as set out earlier. The supervisory manual should also explain how the resulting residual risk will further influence risk-based ICT/cyber risk supervision and oversight activities (see later discussion). Dedicated guidance for onsite examiners—setting out minimum procedures for col-

[7]Often referred to as the Plan-Do-Check-Act cycle or Deming cycle, the concept is the basis of several quality management approaches, including ISO standards, and is particularly suited to managing fast-changing cyber risk. For example, even though the latest ISO 27001 version does not mention it by name, the entire structure of it follows the Plan-Do-Check-Act concept.

[8]The European Banking Authority guidelines on ICT risk assessment show how the assessment of information security or cybersecurity can be integrated into the Supervisory Review process. The guidelines aim to ensure convergence of supervisory practices in Europe and contain concrete guidance for supervisors on how the assess a firm's ICT strategy and governance and a firm's ICT risk exposures and controls. Although cybersecurity is not explicitly mentioned, it is included the broader context of information security (European Banking Authority 2017).

lecting evidence, assessing compliance, and reporting—should complement supervisory manuals.

As a starting point, supervisors must understand the cyber risk profile of supervised firms by assessing relevant threats and identifying vulnerabilities. The assessment of financial systems' general threat landscape informs the assessment of each individual firm's threats and vulnerabilities. When assessing the cybersecurity risk profile of a firm, supervisors should consider all relevant information about the firm's cybersecurity risk exposure. Clear indicators can be defined that help to monitor the potential impact of a significant loss in the availability, integrity, or confidentiality of the firm's critical information. Examples of indicators are (1) the level of internet dependencies of critical ICT systems, (2) the complexity of the general ICT system landscape, or (3) the outdated nature of critical ICT systems. Although all firms face cybersecurity risk, smaller and lower-capacity firms should focus on strengthening cyber hygiene, and the largest and most globally connected firms and key system nodes should be subject to heightened standards commensurate with their size, scale, interconnectedness, and risk profile.

The cybersecurity risk profile of a supervised firm informs the cyber risk control maturity level expected by the supervisor. The higher the exposure of a supervised firm to ICT or cybersecurity risks, the greater the expectation of maturity of controls. For example, identity management is a key control requirement applicable to all financial sector participants, but the way it is implemented can vary from simple manual methods in case of a small securities firm with low cybersecurity risk exposure to sophisticated automated solutions in case of a large firm with a high exposure to cybersecurity risk. In addition, while baseline controls should be implemented by all firms, small or big, additional control measures are expected from firms with a high inherent cyber risk.

Testing the implementation of risk control requirements, as defined in regulation and supervisory manuals, will provide important insights to supervisors. A properly implemented risk control framework can prevent inherent cyber risks[9] from materializing and therefore lay the foundation for ex ante cyber resilience. Critically, supervisors should ensure that supervised firms have strong risk assessment programs in place built on an understanding of information technology assets and their criticality in terms of availability, confidentiality, and integrity. The criticality assessment conducted by the supervised firm can help the supervisor to identify and prioritize relevant threats and vulnerabilities and decide on the effectiveness of existing controls. Generally, supervisors should enforce an enterprise-wide approach to cyber

[9]An inherent risk describes the probability and impact of a loss existing in a business environment in the absence of any action and control.

risk management by supervised firms. The business costs of a potentially successful cyber attack should be considered in risk management planning. As examples:

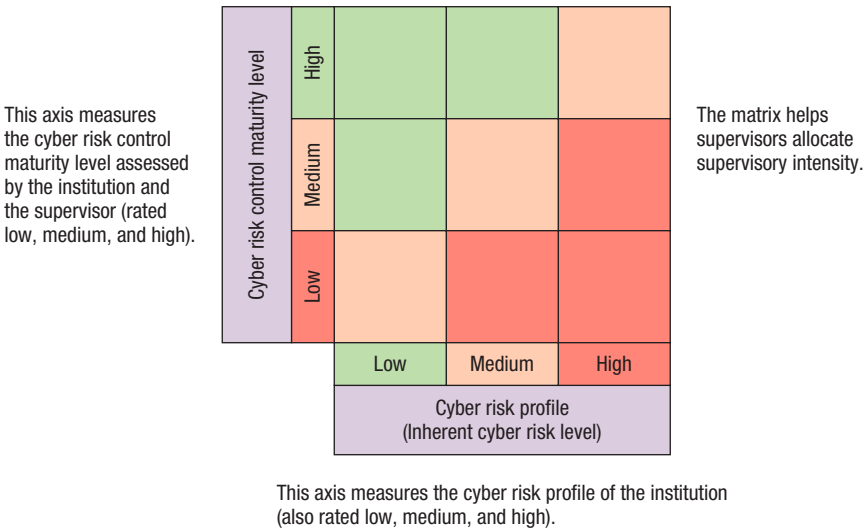
- A cyber attack disrupting the firms' connection to trading platforms and, at the same time, rendering business continuity arrangements ineffective by cutting communication lines could leave the firm with exposures that it cannot manage but which the attacker can take financial advantage or to open positions against which the attacker could trade.
- A cyber attack that grants the attacker access rights would allow the initiation and approval of payments and control over fraud monitoring systems, which could lead to large undetected malicious transactions.
- A cyber attack encrypting all accounting and customer data, including backups, could lead to a significant loss of revenue and goodwill.

Significant residual risks can be a trigger for supervisory measures. Where cyber threats can potentially exploit vulnerabilities of an ICT asset due to an ineffective or missing control, a residual risk exists. Supervisors should be aware of any significant residual cybersecurity risks of a supervised firm and their potential impact on the financial system. The higher the impact on the financial system, the higher cybersecurity risk-control maturity-level expectations should be. As risks are rapidly evolving, supervisors typically expect a control maturity level that exceeds the inherent cyber risk level from critical nodes (Figure 3). Even supervised firms with a low inherent risk might be required to have a medium level of cybersecurity controls in place, for example, where cyber mapping has revealed their criticality for the financial system. Where the control maturity level is below supervisory expectations (pink and red areas in Figure 3), remediation plans addressing deficiencies can help to incentivize fast risk mitigation. Whereas capital add-ons are not a solution for deficient risk management, supervisors may want to incentivize risk mitigation via capital measures. Equally, the inclusion of probable cybersecurity risk–related loss scenarios in the economic capital calculations conducted by the supervised firms themselves should help inform management decisions regarding the need for risk management.

A framework developed by the US Federal Financial Institutions Examination Council (FFIEC)[10] covering the cyber risk profile and cyber control maturity assessment is one example of a standard that can be adopted by supervisors. The framework was developed to help firms identify their risks

[10]The FFIEC was established on March 10, 1979, and is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau. For more information, see https://www.ffiec.gov/about.htm.

Figure 3. Cyber Risk Maturity-Control Matrix



Source: IMF staff.

and determine their cybersecurity preparedness. The assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time. Using the information outlined in the FFIEC's assessment, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security developed the Automated Cybersecurity Assessment Tool to provide all members of the financial services industry with an outline of the guidance and a means to collect and score their responses to the assessment questions (Box 2). The tool is remarkable among published cybersecurity assessment methods because it is specifically tailored for the financial sector. Supervisors considering the tool should adapt it to their jurisdictions, because it is calibrated to the size and maturity of the US financial sector. Once adapted, a similar tool can be used as a self-assessment that is collected, analyzed, validated, and acted upon in the supervisory process. Supervisors should prioritize validation during onsite examinations. A good approach in this regard is to do sample-based effectiveness testing of the declarative statements marked as implemented.[11]

When conducting a cybersecurity risk assessment, supervisors should also be aware of potential risks associated with using third-party providers. In recent years, outsourcing of ICT has increased due to firms' earnings pressure and the drive for efficiency. This movement has not been isolated to traditional technology-based services such as core bank processing, and it may now

[11]Declarative statements in the FFIEC tool are in fact high-level control descriptions that can be tested for effectiveness using well-established audit techniques.

Box 2. US FFIEC Cybersecurity Assessment Tool

Process Flow for Institutions

Step 1: Read Overview for Chief Executive Officers (CEO) and Boards of Directors to gain insights on the benefits to institutions of using the Assessment, the roles of the CEO and Board of Directors, a high-level explanation of the Assessment, and how to support implementation of the Assessment.

Step 2: Read the User's Guide (Updated May 2017) to understand different aspects of the Assessment, the relation between the inherent risk profile and cybersecurity maturity, and the process for conducting the Assessment.

Step 3: Complete Part 1: Inherent Risk Profile of the Cybersecurity Assessment Tool (Updated May 2017) to understand how each activity, service, and product contribute to the institution's inherent risk and determine the institution's overall inherent risk profile and whether a specific category poses additional risk.

Step 4: Complete Part 2: Cybersecurity Maturity of the Cybersecurity Assessment Tool (Updated May 2017) to determine the institution's cybersecurity maturity levels across each of the five domains. This is done by marking all declarative statements as implemented, not implemented, or not applicable. Based on this input the tool calculates the maturity levels across five cybersecurity domains (Cyber Risk Management & Oversight, Threat Intelligence & Collaboration, Cybersecurity Controls, External Dependency Management, Cyber Incident Management and Resilience).

Step 5: Interpret and analyze assessment results to understand whether the institution's inherent risk profile is appropriate in relation to its cybersecurity maturity and whether specific areas are not aligned, and warrant developing a strategy to reduce inherent risk and improve the maturity levels.

include loan portfolio analysis, interest rate risk modeling, or risk management services. Supervisors should ensure that ICT security requirements—including minimum cybersecurity requirements, specifications of the firm's data life cycle, requirements regarding location of data centers, and data encryption requirements—are in line with the supervisor's expectations. Incident handling procedures, including escalation and reporting, should not become ineffective due to any outsourcing or other contractual arrangement with any third party, irrespective of if this party is part of the firm's affiliated group or not.

Supervisors should prioritize the assessment of firm's third-party risk management in on- and offsite supervision programs. There are a multitude of approaches to assessing third-party risk management. Among others, the US Federal Reserve Bank and the European Banking Authority have published detailed expectations on a supervised firm's third-party risk management, and the Basel Committee on Banking Supervision has articulated observed best practices (see Box 3).

To be effective, authorities need to ensure that supervisors have the necessary experience and expertise to conduct effective cyber risk supervision. To assess a firm's cyber risk profile and cybersecurity risk control maturity level, adequate technical skills and an appropriate number of resources are needed. An increasing number of cyber attacks and the rising potential of material losses and business interruptions caused by these attacks has led to increased supervisory and oversight efforts. Globally, supervisory authorities are implementing measures to strengthen specialist and generalist skills on this topic to assess the cyber threats and risks to which the entities under their supervision are exposed. Nonetheless, skills gaps do exist in many jurisdictions. Filling these staffing gaps should be a key concern of authorities, given the impact cyber threats can have for financial stability. The combination of generalist supervisory skills (with an operational risk management focus) complemented with technical specialists (often drawn from staff within a central bank responsible for ICT) have proven to be an effective solution.[12]

Information Sharing and Reporting

Effective information sharing and reporting are essential elements to combat cyber threats. At the domestic level, information on threats, emerging technologies, and other intelligence can be shared among industry participants, as well as between supervisory counterparts and more broadly from a critical infrastructure perspective (Figure 4). Sufficiently detailed anonymized data shared on appropriate platforms help to properly and timely react to cyber threats. In addition, information on incidents and successful attacks should be reported by regulated entities to their supervisors. Trust is the essential element in effective information sharing and cooperation among supervisors and supervised firms. Strengthening trust will support cyber resilience for the financial system as it is increasingly interconnected. Data policies are also crucial underlying elements—data protection requirements should be considered when setting up information-sharing platforms. However, these requirements should not be used as an excuse for not sharing information at all.

[12]This is only correct as an interim measure until a properly skilled dedicated cybersecurity supervisory team can be established.

Box 3. The European Banking Authority and US Federal Reserve Bank's Approach to Supervising Third-Party Risks

The Bank Service Company Act provides US federal banking agencies with the authority to regulate and examine the performance of certain services by third-party service providers to a depositor institution (DI) or affiliate to the same extent as if such services were being performed by the DI on its own premises. Supervision activities have focused on services provided by technology service providers that host or process core banking applications, payments, accounting, and critical data systems with the caveat that the scope of examinations is limited to the services being performed for DI customers.

Outsourcing risk management includes several steps:[1]

- Risk assessment landscape: Identify the service providers and assess their qualifications as well as potential benefits and risks from the point of view of a DI, ensuring that outsourcing is consistent with the institution's strategy and business model (that is, scope, complexity, and importance of outsourced functions).
- Due diligence for the selected service providers: Evaluate the service provider based on the key components—business background, reputation, and strategy, financial performance, operations, and internal controls.
- Assessment of contract provisions and considerations, incentive compensation review, and business continuity and contingency plans.
- Continuous oversight and monitoring of service providers.

The European Banking Authority has been following a similar approach. In its guidelines on outsourcing arrangements,[2] the European Banking Authority goes, however, in even more detail and explicitly covers cloud services. In addition to what is mentioned previously, the requirements include:

- Concrete governance requirements;
- A proper outsourcing policy;
- Assessment of conflicts of interest;
- Business continuity plans covering the failure of a critical service provider;
- Internal audit function;
- Documentation;
- Specific provisions on sub-outsourcing of critical or important functions; on security of data and system; on access, information, and audit rights; and on termination rights;
- Oversight of outsourced functions;

[1]Federal Reserve. 2013. Guidance on Managing Outsourcing Risk, December 2013. https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf.

[2]European Banking Authority. 2018. Guidelines on Outsourcing Arrangements. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.

Box 3 *(continued)*

- Exit strategies; and
- Adequate reporting to supervisors.

National approaches to supervising third parties (as explained previously) are often based on guidance developed by international standards-setting bodies, which have long set expectations for outsourcing in financial services.[3] The BCBS published its "Principles for the sound management of operational risk and the role of supervisors," which lays the foundation for approaches to third-party risk management.

[3]See Basel Committee on Banking Supervision. 2005. The Joint Forum, Outsourcing in Financial Services.

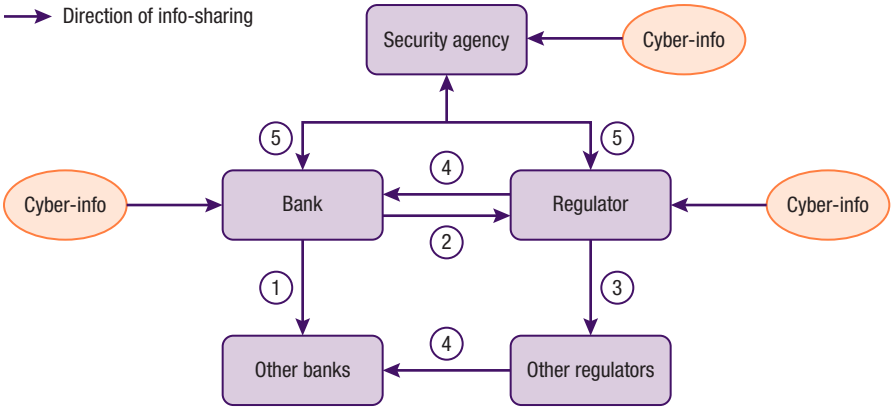
The sharing of information among firms is a key element in strengthening resilience of the financial sector against cybersecurity risks. The G7 Fundamental Elements state, "Given information sharing's importance, entities and public authorities should identify and address impediments to information sharing." Challenges include the need to establish trust, achieve interoperability and automation, safeguard sensitive information, and evaluate the quality of received information. Arguably the main impediment is legal—specifically the fear of legal reprisal. Legal risks of sharing can come mostly from sharing too much or too broadly and failing to act on the information received.[13] Industry-led initiatives have been successful to date, and in the event information sharing between firms is not effective, supervisors could play a role to facilitate effective sharing.

Supervisors should establish clear requirements on cyber incident reporting. Mandatory cyber incident reporting is a fundamental need, and many of the leading jurisdictions have enacted regulation to this end. Reporting requirements should establish a threshold that ensures enough information is reported to focus attention on significant issues, avoiding too much reporting, which in addition to imposing costs also may result in so much information that significant issues are obscured. A threshold could include a combination of factors such as the importance of systems affected (for example, incidents affecting critical systems),[14] the duration of downtime (for example, incidents causing downtime, the type of incident such as a data breach), the internal risk classification of the incident (for example, medium and high), and so on. Further, regulation should specify the required time-

[13]A 2017 survey of cybersecurity professionals in the United States and United Kingdom showed that after lack of threat intelligence experience, the primary reasons why organizations do not share is because of legal concerns.

[14]Criticality in this context is based on supervised firms' own classification.

Figure 4. Basel Committee for Banking Supervision Illustration of Interlinkage of Different Types of Cybersecurity Information-Sharing Practices



Source: Basel Committee for Banking Supervision.

liness of reporting and could limit the scope of firms required to do ad hoc reporting based on their importance in the financial system. International convergence on cyber incident reporting should be envisaged.[15]

In jurisdictions with multiple supervisory authorities for the financial sector, appropriate protocols and platforms should be developed for interauthority information sharing. In addition, authorities should coordinate their reporting requirements, thus laying the foundation of effective sector-wide cyber risk assessments and coordinated countermeasures.

Supervisory authorities could use several mechanisms to address trust and national security concerns. For example, (1) cross-border submissions could be made without naming the source (that is, victims of the attack), (2) actual loss data need not to be shared as an indication of the severity is sufficient, and (3) the submission could be limited to information relevant to detection and response—this clearly benefits everyone without any threat to national security. Additionally, an information classification protocol could be employed to restrict circulation. Consistent adherence to the protocol could be a way to build and strengthen trust.

Role of the Supervisor to Encourage Adequate Response and Recovery

Supervisors play a key role in ensuring that supervised firms are sufficiently prepared to limit the damage wrought by cyber incidents and in ensuring

[15]The Institute of International Finance (2018) has described risks connected to regulatory fragmentation.

that incident response forms a part of ongoing improvements to resilience. Constant attacks, with varying success, are now a permanent feature of the financial landscape, necessitating an emphasis on the ability of firms and the system to respond. Key emphasis should be placed on planning by supervised firms for incident response, business continuity (including robust backup data and systems replicability), and recovery. Cyber risks may put an additional premium on ensuring adequate redundancy across information technology platforms as well as locations, as an attack that affects one data system may not be effective on others. This should include specific consideration of cyber incidents in recovery planning by individual firms, making incident reporting an important part of this process. Procuring cybersecurity liability insurance could also help mitigate potential financial losses.[16]

A focus on response is a priority for two reasons: inevitability of attack and a need to build a continuous link between response and resilience planning. Even institutions with highly sophisticated cyber defenses experience successful attacks. Effective processes for response and recovery are crucial to protect key functions and guarantee their availability in a quick recovery. There is a continuous and dynamic link between resilience capacity and response—for example, systems within an institution that must recover fastest may need stronger defenses. By focusing on response, supervisors will gain key insight into overall operational resilience of the financial system. This insight will then inform how supervisors approach their role in setting standards and supervising their implementation.

Firms need to develop robust business continuity management to minimize negative impacts from operational disruptions. Operational disruptions to firms and markets (including market infrastructures) threaten the viability of firms and cause instability in the financial system (Bank of England 2018). Sound business continuity management will help mitigate potential systemic risks of failure. Firms need to make sure their businesses are resilient to operational disruptions and are designed to resume critical functions rapidly, safely, and with accurate data (CPMI/IOSCO 2016, 16–19).

An in-depth understanding of business continuity plans of supervised entities will help supervisors to respond appropriately in case of an emergency. Dependencies and interconnections need to be clearly understood and tested for resilience in times of stress. Supervisors will need to draw on their understanding of the overall landscape and on the risk assessments by supervised firms. Supervisors can assist firms by helping to maintain awareness of the interdependencies and potential build-up of concentrations in material service providers. Firms should be required to review and test (at least annually) business continuity plans and report the results to the supervisor. These

[16]See Annex 1.

reports should be assessed by the supervisor at the firm-specific level as well as consolidated at a system level to produce a holistic view. Maintaining an up-to-date view of the financial and technology networks will help inform the analysis of business continuity plans. Importantly, supervisors should have a detailed understanding of the most systemically important firms, markets, and products that need to be prioritized for business continuity in the event of a disruption.

Priorities for supervisors regarding response include the following:

- Based on threat analysis, supervisors need to make sure that supervised firms are prepared for probable disruption events originated by cyber attacks.
- Potential impacts need to be analyzed.
- Supervisors need to make sure that bank's recovery time objectives (RTO)[17] and recovery point objectives (RPO)[18] are in line with needs for financial stability objectives.
- There should be one or more fallback data centers at remote sites, at least for the critical activities, services, and resources.
- There should be one or more recovery copies of the critical production data at remote sites.
- Business continuity and disaster recovery tests exist, including simulation exercises.

Supervisors can actively promote the adoption of emerging techniques by financial institutions to improve resilience. Simulation exercises focus on the ability of financial institutions to recover from, and limit the extent of, attacks. This includes a heavy emphasis on ensuring governance structures and decision-making are adequately responsive. Industry exercises should be encouraged and taken forward with the objective of (1) enhancing processes and mechanisms for maintaining shared awareness of cybersecurity threats between authorities and the private sector, and (2) exchanging best practices. Scenario analysis can help institutions understand potential risks, how these may transmit, where investments need to be made, and how best to respond when systems are breached.

Simulated cyber attacks (called penetration tests) have been used by supervised firms for many years to find weaknesses in cyber defenses and using lessons learned to enhance security and resilience. However, the technique has

[17]RTO can be defined as ". . .the time in which the process is intended to be recovered . . ." (German Federal Office for Information Security Standard 100–4).

[18]RPO can be defined as "point to which information used must be restored to enable the activity to operate on resumption" (ISO 22301:2012).

only recently been included in the supervisor's toolkit. With the advent of advanced testing tools and development of professional certification schemes, penetration testing has entered the mainstream of the information security profession, and it is now more feasible for regulators to include it in cybersecurity risk management guidelines and recommendations. The timeliness of these developments dovetails with the increased need to build cyber defenses.

Penetration tests using extreme but plausible scenarios—involving multiple firms, financial regulators, and other authorities—are a key tool in enhancing resilience. In addition to finding weaknesses in systems, these tests assess detection, response, and remediation capabilities of the supervised firm as well as the coordination between participants as a systemwide response to the simulated attacks is developed. These exercises are often called red-team testing.[19] Penetration testing required by supervisors is intended to complement and not substitute private tests organized by firms outside of the supervisory review process.

Supervisors need to strike a balance between costs and benefits when setting minimum expectations for security tests. Penetration tests can become expensive when the scope is broad and advanced techniques are required (such as social engineering or reverse engineering). Smaller firms might be unable to sustain the associated costs. A good approach is to require penetration testing at regular intervals for high-risk and/or internet-facing applications and application programming interfaces (for example, internet banking and mobile banking). Less onerous exercises exist as alternatives to penetration testing and red-teaming—for example, vulnerability scanning or simplified approaches to penetration testing could be explored by supervisors facing cost challenges or other obstacles.

Vulnerability scanning, although not a substitute to penetration testing, can be a cost-effective way to provide assurance over risks stemming from network vulnerabilities. Penetration testing is inherently expensive because of the specialist skills and manual work required. In return it provides the most realistic risk assessment by mimicking actual hacker attacks. Vulnerability scanning is the process of systematically probing computers and devices on a network for known vulnerabilities without attempting to exploit them. It can be done in a stand-alone way or as part of penetration testing, in the latter case usually repeated several times over the engagement. It can be automated to a high degree and is relatively inexpensive while providing reason-

[19]Red-team testing is a complex simulated cyber attack that targets any combination of weaknesses in technology, processes, and people. Typically, there is a red team (attackers, usually external) and a blue team (defenders, usually internal). The blue team drives the detection, response, and recovery processes that the red team tries to evade. Sometimes purple teams are also involved who intermediate or take turns in both attacker and defensive roles.

able assurance over a potentially much broader scope. The downside is that vulnerabilities discovered by automated scanners are not validated for actual exploitability and the false-positives (which are usually many) can overburden the security team. Nevertheless, requiring regular vulnerability scans can be an especially useful element in cyber risk regulatory schemes for jurisdictions that have limited capabilities.

Generally, supervisory involvement in the actual execution of penetration tests or vulnerability scans is not recommended. It is recommended that supervisors set clear expectations and review results but do not become directly involved. The skills required to conduct vulnerability scans and penetration tests are specialized. Having these security reviews undertaken should be the responsibility of the regulated entity itself, potentially engaging reliable third-party service providers. The role of the supervisor in relation to penetration tests should be the following:

- Review the scope of the test and if engaged, for example, to vet third-party service providers.
- Review the parameters of the test to ensure that it is sufficiently comprehensive and aligned with the risk profile of the financial system and the institution.
- Review the results of the test as well as the mitigation strategy and follow-up the closure of gaps identified by the exercise.

Supervisors can play an important role in coordinating industrywide cybersecurity crisis management exercises. In addition to the security reviews conducted by firms, supervisors could seek additional assurance by mandating, coordinating, and monitoring industrywide cyber crisis management exercises. In these exercises, crisis management capabilities of all relevant stakeholders should be tested in a realistic way. Supervisors could start with tabletop crisis management exercises involving systemically important firms to test reaction and recovery capabilities and, crucially, crisis communication protocols. In some instances, other national agencies with cyber risk management responsibilities could take part in these exercises. For example, provided such entities exist, the national cyber intelligence unit generates plausible crisis scenarios, the national computer emergency response team acts as first responder, and cyber crime units follow-up with forensics and attack attribution.

Scenario planning can help identify the need for enhanced recovery and response measures in the case of concentrations or single points of failure. These exercises enhance processes and mechanisms for maintaining shared awareness of cybersecurity threats between authorities and the private sector, and they enhance the exchange of best practices among institutions. Scenario analysis can help institutions understand potential risks, how these

may transmit, where investments need to be made, and how best to respond when systems are breached. However, such simulations should neither lead to unnecessary duplication of efforts nor extensively narrow down the scope of activities institutions consider adequate. Importantly, linking exercises to business continuity will help ensure cybersecurity is more fully integrated into the overall business operations and enterprise risk management framework with Board of Directors and senior management responsibility. Importantly, the exercises can build upon information derived from cyber and network mapping analysis. An aggregate view of the cyber and financial network can enrich the exercises to identify areas that require additional response and recovery measures owing to systemic importance, dependencies, and concentrations.

Recovery expectations require careful consideration and planning. In general, RTOs and RPOs should be based on a comprehensive business impact analysis and risk assessment. In the business impact analysis, firms need to:

- Identify critical processes.
- Assess the consequences over time of not conducting these activities.
- Identify interdependencies and critical service providers.
- Set priorities timeframes to resume critical processes.

However, setting too rigid or strict RTOs and RPOs could be counterproductive in a cyber attack scenario for two reasons: forensic analysis might not be completed, and, without a comprehensive impact assessment, recovery could be based on compromised data or system components and thus the threat not fully eradicated. Whereas financial market infrastructures might need to recover from an incident in two hours as proposed by CPMI/IOSCO (2016), there is a question about the balance between availability and recovering in a safe state.

Preparedness of Supervisory Agencies for a Cyber Attack

Crisis preparedness for when and if a cyber attack becomes a crisis event is an important responsibility of financial sector authorities. A cyber incident can impact financial stability in several ways. The authorities' ability to respond promptly, decisively, and effectively to cyber incidents that impact financial stability will be predicated on a comprehensive set of tools and powers, adequate resources, and efficient procedures. As with other types of risks, responding to cyber incidents that threaten financial stability will require strong legal and institutional foundations that are key elements of any effective crisis management framework. Authorities should continually evaluate and update their crisis plans to reflect changes in the threat landscape and

the changing nature of firms and markets. Regular exercises across the sector, including public and private entities, are a useful way to ensure plans produce desired results.

The crisis management framework involves different authorities responsible for various pieces of critical financial nodes, who must plan and work together should a serious event unfold. Supporting an orderly management of a significant outage of services or an institutional failure depends on communication among authorities and firms, access to data systems, and access to infrastructure of payments and clearing systems. Lines of reporting and succession for strategic functions must be clearly established: crisis management must not depend on specific staff. These measures should be complemented by a crisis communication preparedness plan, which should define the scope of communication in critical scenarios, alternative means, and a strategy for communication internal to the authorities (for transfer of information and for reaching agreements) and for dissemination to the public.

The loss of ICT infrastructure and/or data integrity adds complexity to crisis management and consideration of the potential lack of data should form a key part of crisis planning. Loss of access to data and ICT infrastructure may require consideration of temporary forbearance, as inability to fulfill contractual obligations (paying checks or debts, responding to margin calls, honor securities or derivatives transactions, etc.) due to the ICT system damage should not in every case prompt resolution, at least not until such time that the firm's recovery plan demonstrates being ineffective. Central banks and supervisors will have to consider how to approach the provision of temporary liquidity in situations where, because of data loss, the financial condition of the firm is difficult to ascertain, for example. In absence of these considerations, impending insolvency would be subject to normal course intervention and resolution.

Conclusion

Cybersecurity risk has emerged as a critical issue for supervisors around the world, necessitating an effort to enhance supervision of cybersecurity risk, building on existing approaches to ICT and operational risk. Whereas most financial firms and their supervisors have developed frameworks for managing cybersecurity risk, the business models of criminals are quickly evolving, with more sophisticated tools appearing faster and at lower costs, creating a continuous challenge. The transfer of knowledge across the community of supervisors, especially lower-income and lower-capacity supervisors, will help raise resilience globally. Regulations should leverage established approaches, including those developed by industry, which will help with a convergence of standards. Although all firms face cybersecurity risk, smaller- and lower-capacity firms should focus on strengthening cyber hygiene, and the largest and most globally connected firms and key system nodes should be subject to heightened standards. Authorities should work together to promote a more consistent and coordinated approach that promotes consistency and convergence.[1]

A strong regulatory and supervisory framework should allow supervisors to substantially improve the financial sector's resilience to cyber attack. Whether the regulatory framework is based on principles or rules, the framework must grant supervisors sufficient authority to address cybersecurity risk and allow supervisors to be sufficiently adaptive to the dynamics of the risk. The supervision framework should include a mapping of the financial system, its key technologies, and the interconnectedness among and between the two. Industry standards and firm's own risk assessments should underpin the supervisory program. Incident reporting should be robust and should inform the continuous improvement of resilience. Cybersecurity risk should be

[1]Although regulatory consistency should be a key priority in developing regulations for cybersecurity, differences in approaches across jurisdictions will remain. Over the past two years, regulators around the world have issued over 30 new cyber rules.

incorporated into offsite and onsite processes and into the overall supervisory evaluation of a firm. Understanding the risk of reliance on third-party service providers should be a key priority for firms and regulators. It will be imperative to overcome chronic skills shortages for this work, especially in developing and emerging economy countries. Capacity building can use multiple approaches—acquire specialists, train generalist supervisors, leverage internal resources—and should be expected to be a steady and continuous process.

An emphasis on recovery planning for cyber events is needed. Cyber attacks have become an inevitable feature of daily life for supervised firms, and eliminating attacks and losses is unrealistic. Simulation exercises should focus on the ability of supervised firms to recover from—and limit the extent of—attacks. This includes a heavy emphasis on ensuring governance structures and decision-making are adequately responsive. Industrywide cyber crisis management exercises should be encouraged. Scenario analysis can help firms understand potential risks, how these may transmit, where investments need to be made, and how best to respond when systems are breached.

Increased domestic and international information sharing will improve understanding of the threat landscape and help firms and supervisors improve resilience. Information sharing relies on the development of trust between counterparts and on a common taxonomy. Policymakers should facilitate sharing of good practices across the supervisory community, raising all standards and risk management. Public/private collaboration, which extends beyond traditional regulatory boundaries to include all relevant financial sector agents, should be strongly encouraged.

Annex 1. Cyber Insurance

Cyber risk insurance can add a useful layer of protection for residual risks and provide incentives to improve risk management, but it is no substitute for effective cyber risk mitigation. Cyber risk is a difficult risk to insure due to the nature of the risk and the currently immature understanding of the risk. The role of insurance is to transfer risks from the insured and pool those risks within the insurer. This presumes that an event that results in losses to all or a substantial proportion of the insured population will not occur. For a risk to be insurable, the probability and cost of losses must be able to be estimated within a tolerable range of error, the maximum loss must be specified, claims for losses must be measurable, and the process of underwriting should be economically viable compared to premiums charged and possible losses. All these aspects of an insurable risk are challenged by cyber risk.

Value can be added through the insurance underwriting process where businesses applying for insurance cover undergo an assessment of their cyber risk management practices leading to identification of improvements. Value may also be added in the claims management process when an incident occurs. Insurers will likely assist clients in improved risk management and risk mitigation techniques, as has been seen in other markets where insurers work with their clients to reduce risk and pass on the benefits through reduced premiums. Insurers may refuse to provide coverage if industry standards are not implemented by businesses (Betterly Risk Consultants 2018). An emerging trend in the United States is for insurers to engage external cybersecurity organizations to assist with quantifying risk and for postevent response (Council of Insurance Agents & Brokers 2018).

In addition to insuring cyber risks, the insurance sector itself is exposed to cyber risk through their day-to-day activities including maintenance of

Annex 1 authored by Peter Windsor.

personal data and interconnections with other parts of the financial sector and the technology sector. Insurers gather, process, and keep considerable volumes of data, including personal information of policyholders and beneficiaries. Insurers are linked to other supervised firms, particularly through their investment activities as well as their capital- and debt-raising activities. Insurers also use technology that is common across the financial sector such as software and cloud services. Insurers outsource a variety of activities to service companies and are therefore exposed to potential cybersecurity issues at those companies.

Regulatory frameworks for insurers are diverse around the world, even among major markets. There is variance in the extent to which supervisors prioritize cyber risk in their activities and the sophistication of tools available to address such risks. The International Association of Insurance Supervisors has published an issues paper on cyber risk (International Association of Insurance Supervisors 2016) and is in the process of developing an application paper as well (International Association of Insurance Supervisors 2018). The issues paper demonstrates that there is no uniform practice among International Association of Insurance Supervisors members who responded to a survey and who participated in the development of the issues paper. The issues paper does detail some good practice examples implemented by individual jurisdictions. A concern is that the diversity of supervisory approaches can lead to regulatory arbitrage opportunities.

Public Sector and Private Sector Role in Developing the Cyber Risk Insurance Market

There is a need for improved access to data on cybersecurity incidents and risk models to support the cyber risk insurance market's growth before it can assume a greater role in mitigating residual risks. A key issue for the insurance industry to tackle is the global nature of cyber risks that impede traditional methods of managing accumulation of losses through geographic risk pooling. The cyber risk insurance market is quite concentrated among a few large international insurance groups, and they have access to data on insured risks. Given that insured incidents are a small subset of the total of cybersecurity incidents and this data is held closely by a small number of insurance groups, data on cybersecurity incidents needs to be more widely accessible to improve understanding of the risk and modelling of the risk.

Legal requirements for companies to disclose cybersecurity incidents will enhance data availability and increase focus on the need to manage and mitigate cybersecurity risks through insurance. Approximately 90 percent of the world's cyber insurance market is in the United States, and one of the

drivers of this is said to be the data protection legislation in most states of the United States (Aon Inpoint 2017). It is expected that the European Union's General Data Protection Regulation, which came into effect in May 2018, will lead to greater development of the cyber insurance market in the European Union. Similar legislative developments in other jurisdictions will be positive to the development of a cyber risk insurance market.

The role of government-run insurance pools for cyber risk insurance in mitigating tail risk is an open question. There are parallels with terrorism insurance pools and other pooling arrangements for aviation, nuclear, earthquake, wind, and flood. The potential benefits of pooling cyber risk are increased market capacity, harmonization of coverage, sharing of information about threats and incidents, and facilitating the transfer of cyber risk to reinsurance and capital markets. Drawbacks to pooling arrangements include limitations on market competition and innovation. Limited pricing differentiation based on risk is another pitfall common to many pooling arrangements.

Box 4. Cyber Risk Modeling in the Insurance Industry

As stated in the body of the paper, cyber risk modeling needs to develop to aid in the pricing of the risk through premiums and to model the exposure insurers have to cyber risk through both stand-alone cyber risk policies and silent cyber risk covered in other commercial lines policies.

There are three broad issues that make modeling of cyber risk particularly challenging:[1]

- Available historical data is incomplete and scarce, and it covers only a short period.
- Cyber threats are evolving so past incidents may not be indicative of future incidents.
- Cyber threats are often borderless, meaning risk accumulation is difficult to predict and potentially reduces the benefits of risk pooling.

However, risk modeling companies and the insurance industry are undertaking work to improve data access and modeling techniques. The following developments are examples where industry participants are working toward improvements:

- In March 2018, RMS launched a probabilistic cyber risk model. It estimates losses at different return periods for five loss categories: data exfiltration, contagious malware, financial theft, cloud outages, and denial of service attacks.
- AIR Worldwide has set out a detailed accumulation methodology and, in collaboration with Lloyds, used it in analyzing the impact of outages of cloud computing service providers and impacts on the US economy and insurers.[2]

Lloyd's, AIR Worldwide, and RMS collaborated to develop standard definitions for some common data pertaining to cyber risk insurance.

---

[1]Institute of International Finance. 2017. Cyber Risk Insurance: A Growth Market Adapting to a Changing Risk.

[2]Lloyds and AIR Worldwide. 2018. Cloud Down: Impacts on the U.S. Economy. https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/cloud-down/aircyberlloydspublic2018final.pdf.

Annex 2. Cyber Mapping

Cyber mapping is one approach to assess cyber risk concentrations of the financial system by developing a framework to analyze interdependencies between financial sector firms and information and communication technology (ICT) providers. At a conceptual level, the approach aims to better understand financial and ICT connections between firms in the financial system (including financial market infrastructures) and between these firms and third-party technology and service providers. The concept builds on traditional supervisory approaches to identify concentration risks in the financial network at a system level and adds to this view the cyber network (that is, those elements of ICT that form the underlying infrastructure for all operational processes in the financial network).

The process of mapping the cyber network will help deepen supervisors' understanding of ICT at both a firm and systemwide level. This exercise begins with collecting financial and ICT-related data at the firm level that is used to develop a network model providing an aggregate view of the relevant interdependencies, which can be used to highlight risk concentrations. By integrating cyber and financial maps, this analysis can help study the effects of concentrations and interconnections and their role in contagion during financial crises or a cyber attack. In building the map, supervisors will need to develop their firm-specific knowledge of the role of technology.

The resulting cyber map can be used in two ways. First, it enables the supervisor to better understand the use of technology at a firm level. This will help inform traditional analysis of operational risks such as business continuity and disaster recovery. Second, at a systemwide level, the cyber map helps identify risk concentrations that might not have been visible by analyzing concentrations of just financial exposures. Ultimately, the map for the system will help develop a more complete picture of relationships between systemi-

cally important firms in the financial system and can then be used to estimate the impact of a cyber attack on any of its nodes (see Figure 1).

There are three important questions that need to be addressed in the planning stage of the exercise. First, what should go on the map or what is the scope of the mapping? Second, what network model and underlying data model to use? Third, how to collect relevant data?

Experimental results[1] suggest that, for a more complex financial sector, it can be expensive and time-consuming to build detailed maps. Although these are useful for research, the added value for supervisors is not proportional to the effort. Therefore, constraints should be applied that limit the effort but still allow for a granularity suitable for drawing nontrivial conclusions. For example, the maps could only include important firms of the financial sector,[2] critical ICT systems, and top ICT third parties.[3]

The limiting factors in choosing the network and data models are complexity, availability of data, and the difficulty to integrate financial and ICT maps. For supervisory purposes the better suited models are those that include a lower number of entity types and the entity attributes' values are on discrete empirical scales.[4] However, it is beneficial to define several map layers, such as data flow, organizational dependencies, and technological dependencies. For example, an IMF mapping experiment used the definitions in Annex Tables 2.1, 2.2, and 2.3 as a starting point to develop the cyber map data model.

Data collection is simplified in the approach described. Weights can be derived from market shares, transaction volumes, or some synthetic metric.[5] Key technological and organizational dependencies and connection time criticalities should be available at the firms in scope, for example, in risk assessments, regulatory reports on outsourcing arrangements, or configuration management databases.

The main steps of the mapping are as follows:

[1]Based on information from initiatives at Bank of England, Deutsche Bundesbank, and the IMF.

[2]Importance can be defined empirically in terms of financial indicators and role in the financial system. It is not necessary for this criterion to be the same as the definition of "systemically important."

[3]There are many ICT third parties with a role in the financial system but only a few can cause serious disruptions. For example, a practical limit could be all ICT third parties that are in the top five at any mapped financial sector firm.

[4]This is because the maps do not need to be very precise to highlight the risk concentrations.

[5]It is important to make the distinction between network node weights and connections weights, for which different source data should be used.

Annex Table 2.1. Definitions

Financial services (FS) firms	Central bank, banks, insurance companies, investment funds, stock brokerages
Financial market infrastructure (FMI) firms	Payment system operators, exchanges, CCPs, depositories, information service providers
Finance industry	All of the above
ICT third parties	Hardware and software vendors, cloud service providers, telecom providers, IT service providers
ICT components	Hardware, software, networks, data centers

Annex Table 2.2. Map Layers

Layer	Showing	Remark
Data flows	Financial services firms Financial infrastructure firms ICT third parties	
Organizational dependencies	Financial services firms Financial infrastructure firms ICT third parties	Types: finance industry internal, finance industry–ICT, ICT–ICT
Technical dependencies	Financial services firms Financial infrastructure firms ICT third parties Hardware, Software, Networks Data centers	Influences organizational dependencies

Annex Table 2.3. Items on the Data Flow Map Layer

Item	Attribute	Value
FS firm	Weight	Judgement-based
FMI firm	Weight	Judgement-based
ICT third party	Weight	Judgement-based
Connection	Direction	Unidirectional / bidirectional
	Weight	
	Time criticality	

- Preparation. This includes finalizing the scoping criteria, the attributes for each entity type, the attributes of the connections, and the value set for each attribute. A database is defined and created.
- Data collection. A list of the entities that go on the map based on the scoping criteria is created. Then data for each entity depending on its category (FS, FMI, or ICT) is collected, such as market share, main service providers and their relative importance, data flows to and from other entities, critical information technology systems, and supporting technologies.
- Finding interconnections. Based on the data collected, a list of connections between entities is created.
- Classification. Continuous data is mapped to discrete attribute values. For each entity and connection, the appropriate value is assigned to each relevant attribute.
- Database load. For each layer, the list of entities and connections as well as the attribute values are loaded into the database.

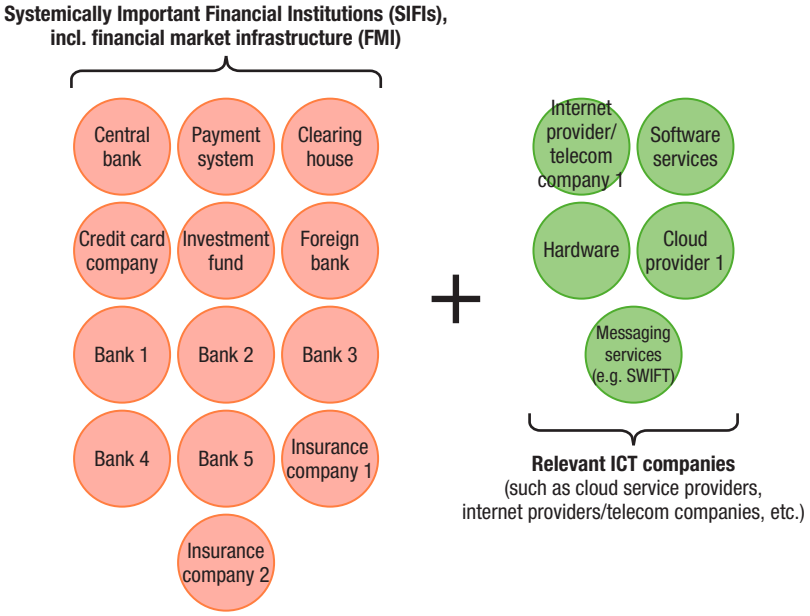
- Visualization. Using appropriate queries, the three layers of the cyber map are programmatically visualized.[6]
- Analysis. Risk concentrations are identified with network analysis tools.

The final output may vary significantly on a country basis, given the heterogeneity of underlying financial structures (for example, bank versus nonbank assets, penetration of market-based mechanisms, organized versus unorganized sectors, etc.), as well as nonfinancial infrastructure (for example, digital versus cash economy, domestic versus international payments). Therefore, any framework will need to be sufficiently flexible to adjust for country and financial sector specificity.

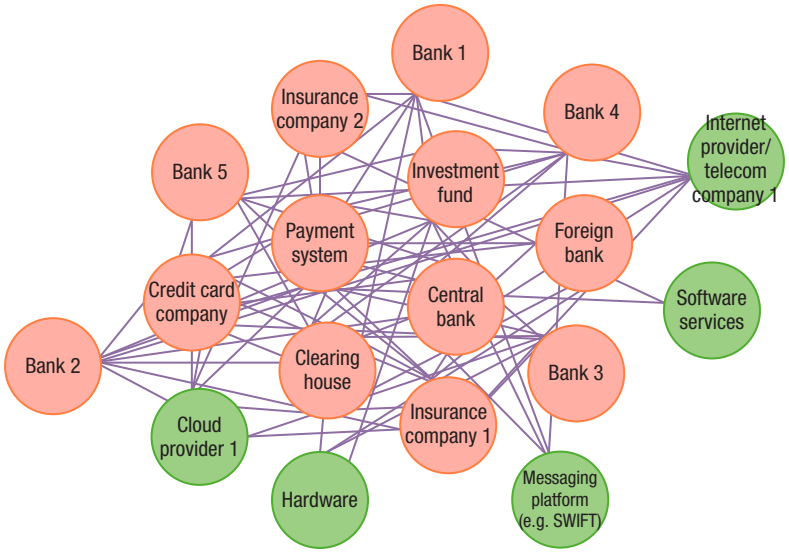
[6]Manual visualization seems daunting. Gephi was used for the stylized visualizations presented in this appendix. Other tools that can be considered are R and Tableau. For the supporting database, Access is more than adequate.

Annex Figure 2.1. Stylized Illustration of Cyber Mapping Process

Step 1: Collect data to develop an inventory of systemically important participants in the financial system and their information and communication technologies networks.

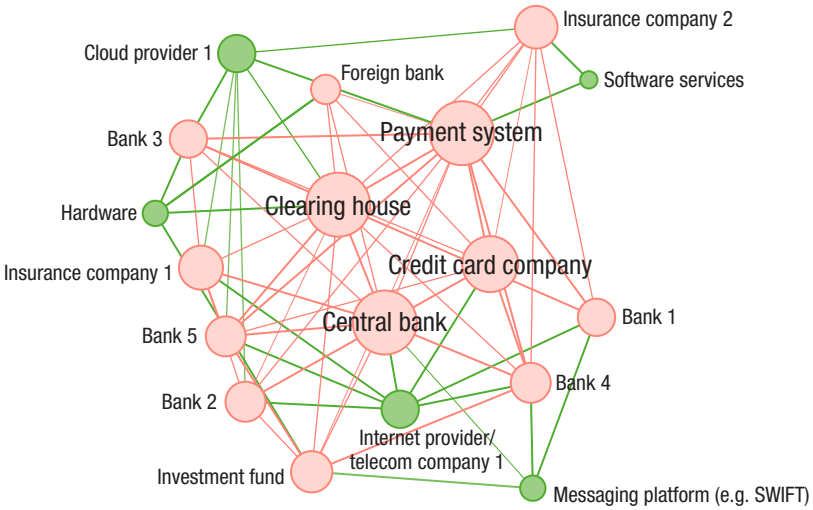


Step 2: Map connections between the participants.

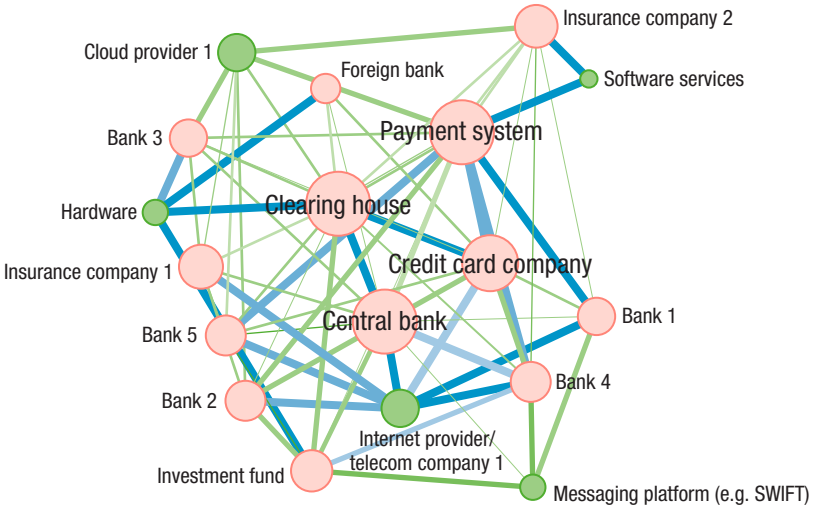


Annex Figure 2.1. Stylized Illustration of Cyber Mapping Process *(Continued)*

Step 3: Adding additional analysis: in this example, degree of centrality measure is used to estimate the size of the node, highlighting the nodes that have more edges, that is, that are more connected. These nodes are critical in the system because they have a high number of interdependencies.



Additional layers can be considered: this map elaborates further by adding weight of the data flow between nodes. The thickness of the line denotes the volume of data transferred between the nodes, providing additional insight. This allows illustration of critical connections in the system and highlights important relationships and dependencies.



Source: Basel Committee for Banking Supervision.
Note: telecom = telecommunications.

References

Accenture. 2017. High Performance Survey Report 2016. https://www.accenture.com/t20170406T052041Z__w__/us-en/_acnmedia/PDF-35/Accenture-Building-Confidence-Facing-Cybersecurity-Conundrum-Transcript.pdf#zoom=50

Aon Inpoint. 2017. Global Cyber Market Overview. http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Bank of England. 2018. Building the U.K. Financial Sector's Operational Resilience. https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

Basel Committee on Banking Supervision. 2011. Principles for the Sound Management of Operational Risk. https://www.bis.org/publ/bcbs195.pdf

———. 2018. Cyber-resilience: Range of Practices. https://www.bis.org/bcbs/publ/d454.pdf

Betterly Risk Consultants. 2018. The Betterly Report: Cyber/Privacy Insurance Market Survey – 2018. https://www.irmi.com/docs/default-source/publication-tocs/betterley-report---cyber-risk-market-survey-june-2018-summary.pdf

Bouveret, Antoine. 2018. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," IMF Working Paper 18/143, International Monetary Fund, Washington, DC.

Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions. 2016. Guidance on Cyber Resilience for Financial Market Infrastructure, 5. https://www.bis.org/cpmi/publ/d146.pdf

Council of Insurance Agents & Brokers. 2018.. Cyber Insurance Market Watch Survey Executive Summary. https://www.ciab.com/wp-content/uploads/2017/05/Spring2017_CyberSurvey_ExecSummary_FINAL.pdf

European Banking Authority. 2017. Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP). https://eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf

Financial Stability Board. 2018. Cyber Lexicon. https://www.fsb.org/wp-content/uploads/P121118-1.pdf

G7. 2016. G7 Fundamental Elements for Cybersecurity. https://www.gov.uk/government/publications/g7-fundamental-elements-for-cyber-security

Information Systems Audit and Control Association. n.d. Control Objectives for Information and related Technology Framework (COBIT). http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-Products.pdf

Institute of International Finance. 2017. Cybersecurity & Financial Stability: How Cyber-attacks Could Materially Impact the Global Financial System. https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767

———. 2018. "Addressing Regulatory Fragmentation to Support a Cyber-Resilient Global Financial Services Industry." https://www.iif.com/portals/0/Files/private/iif_cyber_reg_04_25_2018_final.pdf

International Association of Insurance Supervisors. 2016. "Issues Paper on Cyber Risk to the Insurance Sector." https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

———. 2018. "Application Paper on Supervision of Insurer Cybersecurity." https://www.iaisweb.org/page/supervisory-material/application-papers/file/77763/application-paper-on-supervision-of-insurer-cybersecurity

Kashyap, Anil K., and Anne Wetherilt. 2018. "Some Principles for Regulating Cyber Risk." http://faculty.chicagobooth.edu/anil.kashyap/research/papers/Some_Principles_for_Regulating_Cyber_Risk.pdf

McAfee and Center for Strategic & International Studies. 2018. Economic Impact of Cybercrime—No Slowing Down. https://www.csis.org/analysis/economic-impact-cybercrime

Office of Financial Research. 2016. 2016 Financial Stability Report. https://www.financialresearch.gov/financial-stability-reports/files/OFR_2016_Financial-Stability-Report.pdf

———. 2017. 2017 Financial Stability Research. https://www.financialresearch.gov/financial-stability-reports/files/OFR_2017_Financial-Stability-Report.pdf