December 2020 SDN/20/07

IMF STAFF DISCUSSION NOTE

Cyber Risk and Financial Stability: It's a Small World After All

Frank Adelmann, Jennifer Elliott, Ibrahim Ergen, Tamas Gaidosch, Nigel Jenkinson, Tanai Khiaonarong, Anastasiia Morozova, Nadine Schwarz, and Christopher Wilson

Cyber Risk and Financial Stability: It's a Small World After All

Prepared by Frank Adelmann, Jennifer Elliott, Ibrahim Ergen, Tamas Gaidosch, Nigel Jenkinson, Tanai Khiaonarong, Anastasiia Morozova, Nadine Schwarz, and Christopher Wilson[1]

Authorized for distribution by Aditya Narain and Yan Liu

JEL Classification Numbers:	G18, G28, O33
Keywords:	Cyber risk, financial stability, cybersecurity, financial regulation, operational resilience, risk management
Authors' E-mail Address:	frank.adelmann@gmx.com; jelliott@imf.org; tgaidosch@imf.org; njenkinson@imf.org; tkhiaonarong@imf.org; amorozova@imf.org; nschwarz@imf.org; cwilson@imf.org

[1] This note has benefited from help and input from colleagues Yan Carriere-Swallow, Attila Csajbok; Andrew Giddings, Vikram Haksar, Barend Jansen, Yan Liu, Aditya Narain, Oluwakemi Okutubo, Miguel Otero-Fernandez, and Mario Tamez and from comments received in rounds of internal review. The authors would like to thank Thais Ferreira for excellent administrative support. Frank Adelmann and Ibrahim Ergen co-authored the SDN while serving as members of IMF staff.

CONTENTS

GLOSSARY

AML/CFT	Anti–Money Laundering/Combating the Financing of Terrorism
CPMI	Committee on Payments and Market Infrastructure
CSP	Critical Service Provider
FI	Financial Institution
FMI	Financial Market Infrastructure
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
G7	Group of Seven
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
TA	Technical Assistance
VaR	Value at Risk

EXECUTIVE SUMMARY

The ability of attackers to undermine, disrupt, and disable information and communication technology systems used by financial institutions is a threat to financial stability and one that requires additional attention. Attackers have broad access to technology, allowing them to operate across borders and to attack financial firms and central banks either for profit or simply to disrupt. An increase in the incidence of attacks, rising losses, and the recognition of the potential for serious disruption to the functioning of the financial system has elevated cyber risk from a concern of IT departments to a central risk management issue for all financial institutions and a risk to system-wide stability. Attackers are universal in their reach—targeting large and small institutions, rich countries and the less well-off alike. The COVID-19 crisis has only heightened awareness of the vital importance of protecting digital systems and connectivity to ensure the continuity of economic and financial activity.

Financial systems are at varying states of readiness to manage such attacks, and the international response is fragmented (Lipton 2020). We suggest there are six major gaps that, if addressed, could considerably reduce cyber risk and help safeguard global financial stability[2]. These build on the need to pay greater attention to prevention, mitigation, measurement, and recovery. Addressing the gaps will require a collaborative effort by standard-setting bodies, national regulators, and industry associations, as well as by international financial institutions and other capacity development (CD) providers. The IMF is playing its role by participating in the discussions of regulatory bodies and engaging with other stakeholders to provide CD to its global membership.

Financial Stability Analysis—Better incorporating cyber risk into financial stability analysis through mapping key financial and technology interconnections (cyber mapping), network analysis, and stress testing will improve the ability to understand and thus mitigate risk. Quantifying the potential impact will help focus the response and promote stronger commitment to the issue. Work in this area is nascent—in part due to data shortcomings—but must be accelerated to reflect the growing importance of the risk.

Regulation and Supervision—Enhanced consistency in regulatory and supervisory approaches would reduce costs of compliance and build a platform for stronger cross-border cooperation and information sharing. National frameworks diverge. International organizations have begun to coordinate work on the convergence of regulatory and supervisory practices to deliver greater certainty for internationally active financial institutions. Increased supervisory attention on a global

[2] The terminology in this staff discussion note is drawn from the Financial Stability Board's Cyber Lexicon (see FSB 2018). "Cyber" relates to the interconnected infrastructure of information and communications systems, data, processes, and persons and their interactions. "Cybersecurity" means the preservation of confidentiality, integrity, and availability of this infrastructure; "cyber risk" is the probability and impact of events that jeopardize cybersecurity or violate security or acceptable use policies, whether resulting from malicious activity or not. We focus on malicious activity in this note. See also Carnegie Endowment for International Peace (2017).

level, based on consistent regulation, will help address cross-border risk and promote common approaches to a shared problem.

Response and Recovery—Cyberattacks are now a permanent feature of the financial landscape, and financial institutions are increasingly focused on response and recovery—the ability to repel or limit the attack and to quickly resume operations in the wake of a successful attack. Prevention measures—or "cyber hygiene," such as timely upkeep of software and systems—remain a critical foundation, but more is needed. Improving response and recovery functions nationally will help ensure that cyberattacks do not become financial stability events, and establishing international response and recovery arrangements will strengthen the resilience of the globally interdependent system. Crisis preparation and response at both the national and cross-border levels is still emerging, and the "who to call in a crisis" question often remains unresolved. For developing economies this is an even more serious challenge, necessitating support from the international community.

Information Sharing—Greater sharing of information on threats, cyberattacks, and responses across the private and the public sectors would facilitate much of the necessary work. Yet serious barriers to sharing remain. National security concerns and data protection laws have sometimes undermined the ability to share critical information, and there must be greater effort to develop information sharing protocols and practices that work within these constraints. A globally agreed template for information sharing using a common taxonomy, increased use of common information sharing platforms, and expansion of trusted networks could all reduce barriers to sharing.

Preventing Cyberattacks—Enhancing international efforts to disrupt and deter attackers would reduce the threat at its source. Although the ongoing work on developing information sharing and investigation protocols to strengthen the fight against cybercrime is positive, the work remains unfinished. Without renewed and sustained efforts, the costs and risks to the financial sector will only rise, with developing economies left the most vulnerable.

Capacity Development—Capacity building in developing and emerging market economies can strengthen financial stability and support financial and technological inclusion. Low-income countries are particularly vulnerable to this threat. The COVID-19 crisis has highlighted the decisive role that connectivity plays in the developing world—harnessing technology will continue to be a key development goal and with it a need to ensure that cyber risk is addressed, including by adopting low-cost prevention measures.[3] Capacity development in developing economies must therefore be a priority for international financial institutions and other providers.

The priorities outlined in this note set the stage for concerted action to address these gaps. There is a clear advantage in a scaled and coordinated approach to addressing cyber risk; greater effort at the global level will reduce the overall threat and benefit lower-income countries in particular. It is a small world after all.

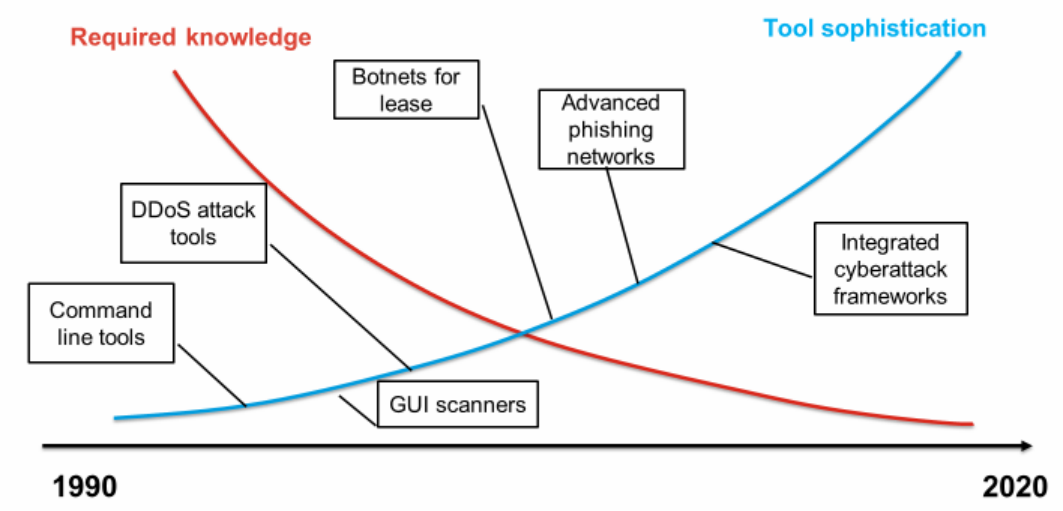
[3] The COVID-19 crisis has given rise to additional cyber risks as a result of greater reliance on remote working and mobile banking. See Adelmann and Gaidosch (2020) for a discussion and guidance on the challenges raised.

CYBER RISK AS A THREAT TO FINANCIAL STABILITY

A. Growing Risk

1. **Attacks on information and communication technology systems (cyberattacks) are rising globally, and financial services continue to be the most targeted industry.**[4] Use by criminals ("cybercrime") has become more widespread—there is a relatively low risk of prosecution and widespread availability of easy-to-use attack tools and cybercrime support services. Advances in technology have provided additional opportunities for attackers as well as for financial institutions aiming to prevent and mitigate the risk. Hacking tools have evolved over the past two decades and can now be used by relatively low-skilled attackers at a fraction of the previous cost (Figure 1). This has led to a sharp rise in the number of cyber incidents and data breaches (Figure 2).

Figure 1. Evolution of Cyber Risk

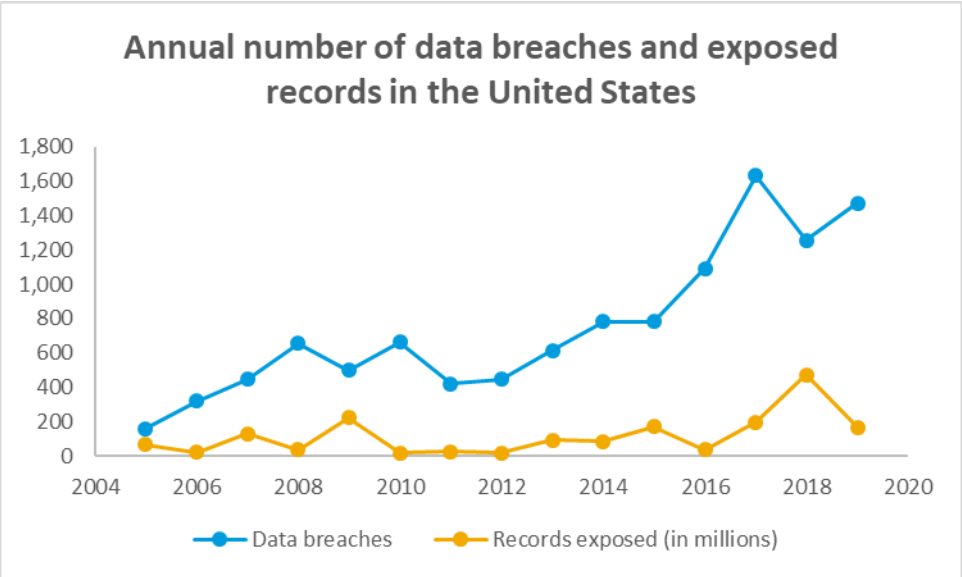


Source: Carnegie Mellon University.

Note: DDoS = distributed denial of service; GUI = graphical user interface.

[4] For example, *Forbes* reported in 2019 (see Doffman 2019) that more than 25 percent of all malware attacks hit banks and other financial services organizations, more than any other industry.

Figure 2. The Rising Number of Cyber Incidents

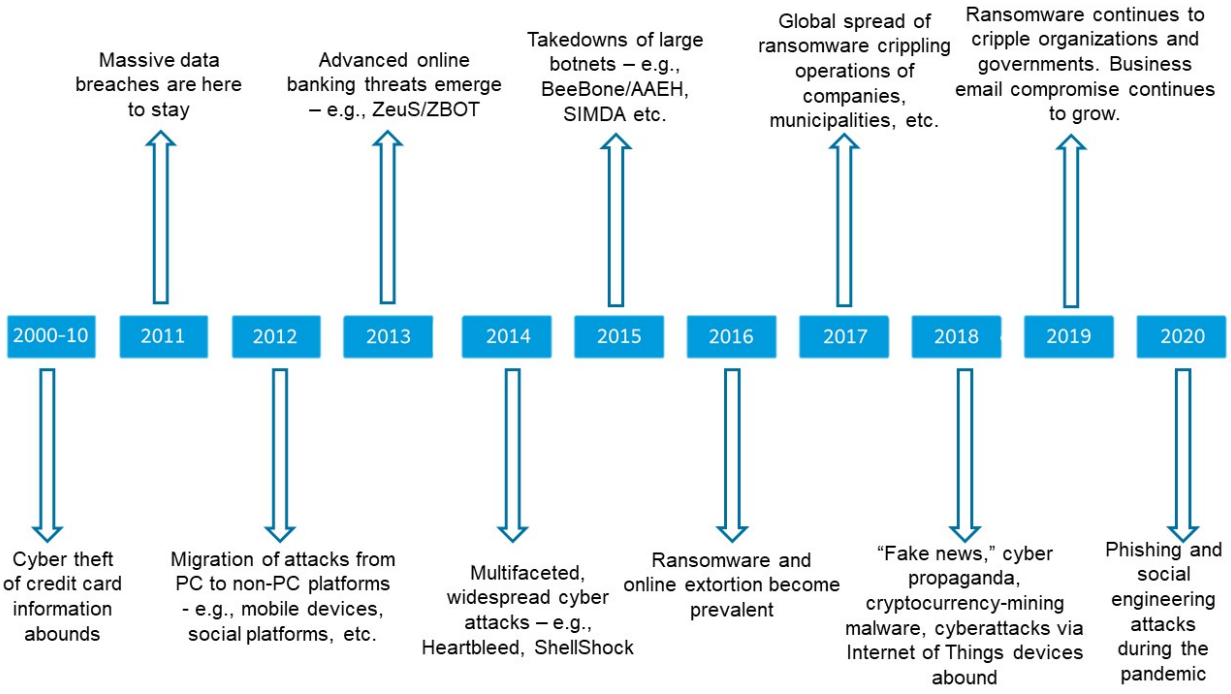


Source: Identity Theft Resource Center.

2. **Cyber threats have become more sophisticated and typically span several jurisdictions, making them harder to investigate and prosecute.** Cyberattacks have been industrialized—for many operations there is an international division of work; there are markets for hacking services, vulnerability exchanges, specialist operators, and outsourcing service providers. Attackers show a degree of agility in cooperation across borders that authorities find difficult to match.

3. **While most attacks are financially motivated, rising geopolitical tensions also increase the risk of disruption-motivated incidents (Figure 3).** Financial services are vulnerable to a wide range of attackers, from lone hackers to sophisticated organizations and nation-state cyber warfare units. The financial sector's reliance on data increases the vulnerability and the complexities of cybersecurity. Data corruption—sometimes also referred to as "data poisoning"—is an emerging additional threat in which the cyberattack feeds bad or misleading data into systems. As with the introduction of disinformation through "fake news," the most worrisome aspect of such attacks is the undermining of confidence. The advent of machine learning and artificial intelligence makes this risk even more relevant should undetected corrupted data be fed into algorithms and used in decision-making.

Figure 3. Evolution of Cyberattacks, 2010–20



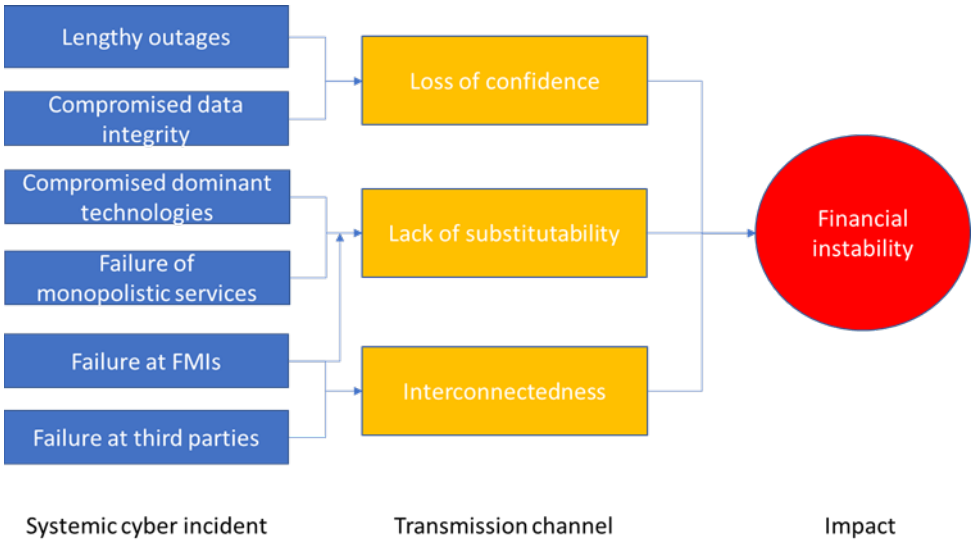
Source: IMF staff illustration.

B. From Cyberattack to Financial Stability Risk

4. **Cyber risk can impact financial stability through loss of confidence and lack of substitutability and interconnectedness.**[5] Figure 4 illustrates the causal chain from cyberattack to financial instability, highlighting the most common root causes and likely transmission channels, although of course alternative combinations are possible. We observe that—with some notable exceptions—most successful cyberattacks affect one institution and produce limited damage. A successful attack with enough technical force to disable or disrupt a key institution or spread through the system could, however, become a systemic event.

[5] OFR Viewpoint 17-01 (Office of Financial Research 2017) identified the following three channels: loss of confidence, lack of substitutability, and loss of data integrity. However, loss of data integrity is a technical issue that leads to loss of confidence and thus is not a direct transmission channel.

Figure 4. Cybersecurity and Financial Stability Channels



Source: IMF staff.

Note: FMI = financial market infrastructure.

Loss of Confidence

5. **Lengthy outages and compromised data integrity can lead to a loss of confidence.** If a widespread attack paralyzes critical operations for an extended period, it may eventually lead customers and market participants to lose confidence in the financial system, making them reluctant to extend liquidity or credit, thereby causing further damage. Attacks and outages affecting one firm may lead to the conclusion that other firms are similarly vulnerable. For example, in the week following the announcement of the Equifax data breach in the United States in 2017, the firm lost 35 percent of its stock value.[6] Although similar firms TransUnion and Experian did not report data breaches, market contagion triggered a 13 percent and 6 percent drop in their equity prices, respectively.[7] Similarly, the disruption of New Zealand's stock exchange in 2020 due to a series of cyberattacks led to a loss of confidence; the trading system remained technically operational, but trading had to be stopped because of concerns about market integrity.[8] Under extreme scenarios, investors and depositors may demand their funds or try to cancel their accounts or other services and products they regularly use.

[6] LaVito (2017).

[7] Gray (2017).

[8] On August 26, 2020, a large distributed denial of service (DDoS) attack affected the New Zealand stock exchange (NZX) network connectivity, and the NZX decided to halt the market in order to maintain market integrity. See https://www.nzx.com/.

6. **Liquidity is likely to be affected quickly if confidence is lost.** System outages and severed communication links can prevent otherwise financially healthy institutions from accessing funding or assets, which would impair their ability to manage exposures and conduct lending and other operations, with the potential for solvency concerns. If the attack compromises the pricing of securities, it will have a system-wide impact (Boer and Vasquez 2017). A simultaneous attack on several institutions could, for example, disrupt safeguards in clearing and settlement systems, resulting in a halt in trading. Recovery of data, moreover, can be complex, and questions about the accuracy of the recovered data could mean that the problem continues over a lengthy period of time.

Lack of Substitutability

7. **The loss of a key service—without easy substitution by other service providers—is another channel through which cyberattacks can affect financial stability.** In many financial systems, one or two large institutions may provide critical services such as custodial or clearing services, which if impacted in an outage would have repercussions in the rest of the sector. Large institutions that dominate interbank markets or institutions that provide niche services and—in developing economies, correspondent banks—may pose substitutability risks. For example, a systems outage at a key financial market infrastructure (FMI), such as a payment system, could disrupt transaction processing, with a chain effect across the system (see Appendix I for a more detailed discussion of the criticality of FMI).

8. **Weaknesses in technology used across the industry can expose many institutions to threats simultaneously and have a broad effect on the entire financial sector.**[9] Finding alternative technologies is often difficult and expensive, as is evident, for example, in the long life cycles of infrastructure and business software used in banks. The consolidation of the information and communication technology sector increases this difficulty. Appendix II considers potential approaches to third-party outsourcing in detail.

Interconnectedness

9. **Interconnectedness—within the financial system and across technologies—also increases the financial stability risk arising from cyberattacks.** Financial institutions transact bilaterally and through trading, settlement, and clearing platforms; the central bank; and payment systems. Institutions are also linked through lending and counterparty risk. An outage in one institution may cause difficulties for counterparties, leading to liquidity problems across the system. For example, in a real-time gross settlement system several banks may rely on incoming payments from a major participant, which if incapacitated can put pressure on intraday liquidity. The financial sector is heavily dependent on data and relies on common data sources, enhancing interconnectedness. Data integrity concerns may call into question a chain of transactions—particularly since the inception of the breach may not be easy to pinpoint. Even if only one

[9] While not a result of a cyberattack, the Google Cloud outage in 2019 is an example of how an operational risk incident can affect wide swaths of the digital economy (see Barrett 2019).

institution is directly affected by an attack, the interconnections in the system may spread the impact more widely.

10. **Technology interconnectedness—exposure to common hardware and software packages, as well as common technology service providers such as cloud services—may also exacerbate contagion risk from cyberattacks.** Cyberattacks can propagate not only through third-party technology service providers but also through targeted clients, retail partners, or counterparties. The cross-border nature of both financial and IT services also raises the risk of cross-border contagion from large-scale cyberattacks.

ENHANCING CYBERSECURITY IN THE FINANCIAL SYSTEM

11. **Mitigating cyber risk in the financial sector is a key public policy objective.** The digitalization of the financial sector has led to even greater emphasis on cyber risk, which is now a priority for private financial institutions—chief executive officers often cite this risk as among their top three concerns. But there is also clear public interest in managing cyber risk across the financial sector, especially since a successful cyberattack has the potential to jeopardize financial stability. Crucially, although financial institutions have clear individual incentives to invest in protection, absent regulation and public policy intervention, they will tend to underinvest from the perspective of society and the broader financial system interest—for example, they will not take into account the impact of their failure or a broader attack on the system as a whole (Kashyap and Wetherilt 2018). While much is being done, we set out below areas where we see a need for further work, with emphasis on the official sector's role.

A. Financial Stability Analysis and Cyber Risk

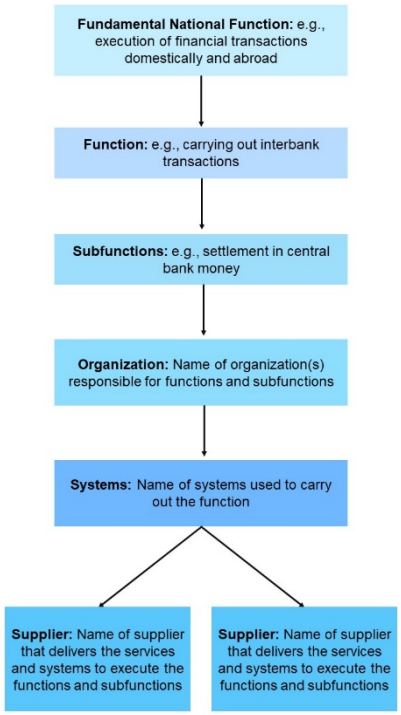
12. **Further improving the identification of major sources of system-wide cyber risk and the potential impact on financial stability will strengthen risk mitigation.** Cyber risk is now commonly highlighted in financial stability reports published by central banks and prudential authorities, although there is significant scope to improve both the quantification of risks and the integration of cyber risk into broader financial stability analysis. Tools are emerging to allow authorities to better understand the nature of the systemic threat and its potential impact. We outline below three such tools that could be widely adopted.

Cyber Mapping

13. **A "cyber map" identifies the main technologies, services, and connections between financial sector institutions, service providers, and in-house or third-party systems.** At a conceptual level, mapping aims to highlight key financial and technological connections between financial institutions (including FMIs) and between these firms and third-party technology and service providers. Even a basic map will identify systemic institutions, service providers, and technology providers and their relationships in the financial system (Figure 5) and thus provide a

valuable reference for supervisors to identify key vulnerabilities and allocate resources.[10] As an example, Norges Bank produced a map of the Norwegian financial sector that sets out fundamental functions. Based on these functions, critical objects, infrastructures, and information systems have been defined at the national level. Sectoral agencies have then added further detail to the initial map, which is used to inform both supervision and financial stability analysis (IMF 2020).[11]

Figure 5. Elements of a Simple Financial Sector Map



Source: IMF staff.

14. **The dynamism and complexity of the financial sector and the technologies it uses can make cyber mapping challenging.** It can be expensive and time-consuming to build detailed maps. However, mapping exercises that do not aspire to completeness and apply thresholds for inclusion, as well as qualitative approaches, have proved to be a useful tool.

Quantitative Analysis

15. **Accurate quantitative estimates of potential losses could usefully inform both firm risk management and financial stability analysis, although producing reliable estimates is difficult and remains a work in progress.** Difficulties stem in part from the limited availability of data on the

[10] See Gaidosch and others (2019), Appendix 2, for more details.

[11] IMF (2020).

frequency and loss severity of cyberattacks. Moreover, even if complete data on historical losses were available, the rapidly evolving nature of cyberattacks and the threat landscape would still pose a challenge to accurate estimation of potential future losses. Distributions of losses from cyberattacks are also characterized by heavy tails, which complicates formal statistical analysis. A promising development in measuring losses as a result of cyber risk is the new operational risk framework of the Basel Committee, which could motivate more banks to collect operational risk data, including on cyber risk.[12]

16. **Against this backdrop, improving the quality and availability of data on losses from cyberattacks, as well as further development of modeling techniques, would help support risk management, supplementing qualitative approaches that rely heavily on expert judgment.** At the firm level, the total costs of cyber incidents include a wide range of direct and indirect elements, with indirect costs typically accounting for the majority. Direct costs (those that can be specifically traced to the occurrence) are incurred early and over a relatively short time period. Indirect (or hidden) costs are incurred over a longer time period and are more difficult to attribute and quantify. These include declines in future revenue, lost productivity, devaluation of trade name, increased borrowing costs, and so on. Insurance does not cover such costs, which compounds the problem. Although the cost is difficult to quantify, industry research suggests that total costs have ballooned in recent years. For example, a recent Accenture study puts the average yearly cost of cybercrime for larger organizations at $13 million, a 72 percent increase over five years (Accenture 2019).[13] In addition, a recent study from Aldasoro and others (2020) found that losses from cyberattacks are still only a small portion of operational losses, but can account for a significant share of total operational value at risk (VaR).

Stress Testing

17. **Stress testing of cyber risk offers promise as a tool to support supervisors and policymakers. Under such approaches, financial institutions are typically asked to assess the impact of cyberattacks on liquidity and capital.** These tests generally involve institutions estimating losses from a prescribed scenario and supervisory review of financial institutions' procedures and coverage against cybersecurity risk. Cyber risk scenarios could also be included in the stress testing and network analysis of FMIs (Heijmans and Wendt 2020). Such exercises encourage financial institutions to further develop their risk management practices in this area. As an example, the Monetary Authority of Singapore conducted a firm-level cyber risk survey as part of the 2019 IMF Financial Sector Assessment Program, which included quantitative estimates of potential losses, among other matters. On average, banks estimated that losses from a direct cyberattack would amount to about 35–65 percent of quarterly net profits, depending on the cyber scenario type, and would cause the Capital Adequacy Ratio (CAR) and the Liquidity Coverage Ratio (LCR) to drop by 0.1–0.4 and 8.4–35 percent respectively (Goh and others 2020).

[12] Formerly, only banks that adopted the advanced measurement approach had to collect operational loss data.

[13] The study covered 355 companies with a minimum of 5,000 employees in 16 industries across 11 jurisdictions.

18. **Comparatively, cyber risk quantification at the systemic level is at an earlier stage of development.** This is an active area of financial stability analysis. Although there are large uncertainty margins around current estimates, these are likely to narrow as data and modeling approaches continue to improve. Estimates of potential losses are high. For example, through Monte Carlo simulations, Bouveret (2018) estimates the 95 percent VaR loss to be $147 billion for financial institutions globally (14 percent of global net income). Bouveret conducts a further experiment in which the mean cyberattack frequency is set to two times its historical peak. Under this scenario, the 95 percent VaR loss rises to $352 billion (34 percent of net income).

B. Regulatory and Supervisory Frameworks

19. **Cybersecurity regulation and supervision play an important role in strengthening resilience and delivering public policy objectives.** Regulation and supervision set consistent minimum standards to be used by financial institutions, including promoting good cyber hygiene and setting expectations for risk management practices, incident reporting, and response and recovery protocols, as well as internal governance procedures. Active financial supervision supports effective implementation (Gaidosch and others 2019).

20. **Good progress has been made to strengthen cybersecurity regulatory requirements, but fragmentation within and across borders causes inefficiencies.** National requirements typically incorporate internationally recognized technical standards[14]—requirements governing how to deal with the technology itself. But there are currently often differences in the transposition of the technical standards into national frameworks. While certain differences in requirements may be justified, fragmented control environments may complicate cyber risk management and drive compliance costs up, particularly for international financial institutions. It is not uncommon, for example, for large international banks to be required to comply with many cybersecurity regulatory requirements that differ slightly but in essence reflect the same control concept. Different industries within the financial sector—for example, insurance and securities—can also be subject to different requirements, which further complicates compliance for large entities active in several industries. Enhanced consistency and convergence among the approaches nationally and internationally would free up resources that could be spent more effectively on managing and responding to risk.

21. **Efforts to address fragmentation and promote harmonization are underway, but convergence is a slow process, and smaller jurisdictions may be left behind.** The Group of Seven (G7), Financial Stability Board (FSB), and Committee on Payments and Market Infrastructure–International Organization of Securities Commissions (CPMI-IOSCO) have published well-known high-level principles. The Basel Committee on Banking Supervision is working on additional

[14] There are many broadly accepted standards for the technical aspects of cybersecurity that can and should be relied on by regulators. The standards most accepted and used globally include International Organization for Standardization (ISO) series (that is, ISO 270xx series); National Institute of Standards and Technology series (NIST—that is, NIST 800 series); Control Objectives for Information and Related Technology (COBIT); and sections of the Information Technology Infrastructure Library (ITIL). These standards are used across all industries. Most financial institutions use a mix-and-match approach by deriving internal policies and procedures from a range of international standards and national regulatory requirements (themselves often derivatives of these global standards) to best address their risk profile and risk tolerance.

principles on operational resilience. In practice, these guidelines have formed the basis for development of national standards for most of the larger and more sophisticated jurisdictions. For jurisdictions that do not participate in these formal standard-setting bodies, however, progress has been more limited, and many jurisdictions have yet to finalize the drafting and implementation of cybersecurity regulations. Lack of technical capacity and experience in transposing high-level principles to suit local circumstances is the most common challenge.

C. Response and Recovery—Cyber Resilience

22. **Cyber resilience[15] has emerged as an important concept in cybersecurity.** While strong cyber hygiene and preventative actions remain important, past assumptions that cyberattacks can be repelled or are relatively rare have given way to the reality that such attacks are a continuous threat and that many will have a degree of success. As the sheer number of incidents rises, both industry and supervisors have refocused from zero tolerance of successful breaches of institutions' systems toward a more pragmatic approach that concentrates on containing the problem and maintaining operations.

23. **Industry and regulators are enhancing their capabilities to take action after a detected cybersecurity incident (response function) and to restore any impaired systems or services (recovery function).** Financial institutions are strengthening internal response and recovery protocols that help maintain critical business functions during disruptions; such preparations also reduce incentives for those seeking to disrupt operations. Adding to this, supervisors have started developing protocols that take an industry-wide view of critical financial services to ensure that operations are maintained or can recover quickly to avoid undue disruption.[16] Supervisors play a key coordination role in response—they are uniquely positioned to identify and observe incidents across financial institutions, are able to share information broadly across the sector in a timely manner, and have a critical role in restoring and maintaining public confidence, including through communication. Emerging market and developing economy countries face challenges in this process, however (Box 1).

Box 1. Cyber Resilience in Emerging Market and Developing Economy Countries

Cyber resilience requires an ongoing effort for all countries, but for developing economies the challenges are particularly daunting. Some of the most high-profile cyberattacks have been in developing and emerging economies—for example, the attacks on the Bangladesh Bank and on banks in Chile and a malware attack on Boleto Bancário, a money order payment system in Brazil. The global cybersecurity skill shortage in both the private and public sectors is rising—there were more than 4 million unfilled positions globally in 2019, up from just less than 3 million in 2018. Per capita, the shortage is most acute in low- and

[15] Cyber resilience is an organization's ability to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents.

[16] To this end, the FSB's work on cyber incident response and recovery can provide a common baseline of effective practices for the industry and regulators alike. See FSB (2019a) or the more recent FSB (2020).

middle-income countries,[1] because of a lack of specialized university courses, less competitive salary structures, and limited access to international expertise. In addition, these countries may have small budgets for advanced cybersecurity technologies that can help identify, protect, detect, recover from, and respond to cyberattacks. Further, there is a risk that, as advanced economy countries become more resilient, attackers will target small and vulnerable nations.

Successful cyberattacks can have far-reaching consequences for developing economies. Outages can have profound effects on the functioning of the financial sector and financing of the real economy, and developing economies are less able to weather such storms. Without the ability to respond and recover, a developing economy is more likely to have a prolonged outage, with potential damage to confidence in the financial system more broadly. International programs, such as the SWIFT Customer Security Program,[2] aim to help participants achieve a cybersecurity baseline. However, given generally limited resources, further initiatives, such as expanded technical assistance, are needed to address the widening cyber resilience gap between higher- and lower-income countries.[3]

Facing these challenges will demand resources from financial institutions and the official sector alike. In the wake of the Bangladesh attack, SWIFT (the international financial messaging system that was fraudulently used in the attack) developed a set of cyber hygiene standards and implemented them globally. The Carnegie Endowment for International Peace developed an online toolkit designed for low-capacity environments. The UK Foreign and Commonwealth Office sponsored an exercise for crisis-management testing with African central banks, and the Bank of France has instituted workshops on cybersecurity for more than 80 countries. The IMF, the World Bank, and the Inter-American Development Bank now have capacity development programs, including an annual global workshop at the IMF for low-income countries supplemented by regional workshops and bilateral assistance. But needs continue to grow in this area, especially as low-income countries try to close the digital gap within their societies and provide greater access to payment services and other financial technologies. It will be important to support cyber risk mitigation as a means of ensuring continued financial stability and integrity, to protect assets in economies less able to absorb loss, and to underpin confidence in new and emerging technologies. Since one of the major causes of inadequate cybersecurity is the dearth of qualified expertise, a promising approach is to encourage and support formal education and professional certification in cybersecurity.

[1] (ISC)[2] 2019.

[2] See more details at https://www.swift.com/myswift/customer-security-programme-csp.

[3] An indicator of the widening gap is the increase in the relative incidence of successful attacks against financial institutions, including central banks, in lower-income jurisdictions, compared with those in advanced economies.

24. **Strengthening the cross-border aspects of response and recovery arrangements is a top priority.** Financial institutions are often connected across borders—through parent institutions, subsidiaries, counterparties in other jurisdictions, correspondent banks, and FMIs—and their ability to respond to and recover from attacks may rely on conditions or actions taken across borders. Very little infrastructure is currently in place to allow for necessary cooperation and information sharing to plan and implement effective response and recovery internationally.

25. **Cybersecurity exercises are very effective resilience assessment tools for financial institutions and supervisors alike.** These exercises are planned events during which an organization simulates a cyberattack that disrupts operations and tests capabilities (for example, prevention, detection, mitigation, and response and recovery). An extension is "red-teaming," which is designed to help entities test and improve their resilience against cyberattacks by employing actual hacker methods to breach or circumvent defenses. Cybersecurity exercises can identify gaps in operational resilience of institutions and of financial systems, helping to identify priorities that strengthen response and recovery capabilities. Exercises can also point to gaps in information sharing arrangements and support collective action to address them.

D. Information Sharing

26. **Information is the lifeblood of risk mitigation and is the basis for risk management and supervisory frameworks.** Pooling information on cyber risks can enhance situational awareness, help detect new risks, and build better responses. Sharing information also reduces the cost of collection for all participants, including the financial sector.

27. **There are currently, however, significant barriers to sharing—most importantly regulatory barriers and concerns about liability.** Limitations on information sharing, particularly across borders, can increase vulnerabilities because information silos can be exploited by cyberattackers, who are able to work across jurisdictions with ease.

28. **Information sharing in the realm of cybersecurity includes the following:**

- Threat Intelligence Information—Information on the source and nature of threats, including which groups may be targeting a specific set of institutions, the technology being targeted or used, and the intention behind the attacks. Threat intelligence information can also include high-frequency alerts, risk analytics, indicators, threat assessments, and analysis. This information gives financial institutions and supervisors a basis for monitoring and addressing vulnerabilities. Such information varies in depth and specificity and is typically shared on a continuous basis between trusted sources.

- Incident Reporting— information on the success of the incident and how it was addressed and may include loss information. Supervisors usually require reporting of incidents with an account of how the financial institution is managing the situation.

- Good Practices—Information on how cyber incidents are reported and analyzed, what incident response has been taken, and what the consequences have been. Good practices also extend to how resilience is being built in institutions through the financial system or how the supervisor is addressing the risk.[17]

[17] It is recognized that regulated entities have broad and extensive reporting and information sharing responsibilities and requirements in both business-as-usual circumstances and during periods of stress; for example, in relation to

- Defense Techniques—information on how an attack was prevented or contained, which may be shared at a technical level.

29. **There are three broad channels of information sharing within the financial sector, and they are at different levels of maturity:**[18]

- Private Sector Institution to Private Sector Institution—The sharing of cybersecurity threat intelligence information between financial institutions within domestic financial sectors is well advanced in many financial systems, including among large global institutions. Sharing may be on an informal basis, such as through personal relationships between chief information security officers or on a more formal basis—for example, via multilateral platforms such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), which originated in the United States but now has global membership.[19] Information is typically shared on a continuous basis in a trusted network and is highly valuable given its relevance to risk managers.

- Private Sector Institution to Public Agency—Private financial institutions typically provide incident reports to their supervisors. Routine protocols for regulatory reporting, as well as the trusted relationship between supervisors and institutions, help support this exchange.

- Public Sector to Public Sector Agencies—Financial supervisors may share incident reports and regulatory responses with other domestic agencies or with cross-border peers. Examples typically include sharing incident information between home and host supervisors.

30. **Smooth sharing of information will require management of legal and reputational risks.** Data are often protected by privacy regimes or national security frameworks, depending on the nature of the underlying information and the parties that are sharing. While most reporting regimes for cyber incidents provide some form of safe harbor for liability related to the incident itself, they generally do not protect the disclosing party from exposure of personal information, and it can be difficult to disentangle information on the incident from customer data, for example, which may entail some residual liability. Many aspects of information—in particular information that reveals vulnerabilities in an institution or information that is related to national security—can be sensitive and raise legal, security, and practical considerations. These sensitivities constrain information sharing between institutions, between financial institutions and national authorities, and, ultimately, international cooperation between national authorities. Financial institutions may

cybersecurity events such as a breach. The discussion focuses specifically on information sharing as it relates to cybersecurity.

[18] This is an oversimplified presentation of information flows in the financial sector. In reality, there are many more channels, such as national security agencies, domestic critical infrastructure providers, third-party service providers, cybercrime agencies (domestic and international), and so on. Nonetheless, for simplicity the discussion has been significantly narrowed to support more concrete policy recommendations for financial sector agencies.

[19] The FS-ISAC is a private sector information sharing platform that offers intelligence, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cybersecurity threats.

also fear reputational risk arising from a successful cyberattack and may be reluctant to share information on any such incident.

31. **The purpose of an information taxonomy for cybersecurity is to develop a structured approach to information and intelligence sharing.** Once a taxonomy of cyber information is developed, other questions, such as " why share, what to share, who to share with, how to share, and when to share" can be more effectively answered (Table 1). [20]

Table 1. High-Level Categorization of Information Sharing

Categories of Information	Examples
Information that cannot be shared	Information sensitive to national defense concerns—e.g., cyber warfare related
	Personally identifiable information
Information that could be shared	Details of cyber threats in near real time and approaches to defense; intelligence sharing
Information that should be shared	Situational awareness, risk management practices, technical vulnerabilities, patches, etc.

32. **Promoting trusted information sharing among private and public institutions can help overcome resistance.** Platforms where threat intelligence is shared on a continuous basis establish efficient and long-standing relationships that build trust. For example, the FS-ISAC has developed a network for central banks, regulators, and supervisory authorities (the CERES Forum)[21] for members to receive timely, targeted information; tools and resources about cybersecurity threats; and threat mitigation strategies. Other examples of international arrangements for information sharing include those in place for SWIFT and the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) Cyber Information and Intelligence Sharing Initiative.[22] Data sharing also

[20] The Federal Reserve Bank of Richmond organized a cyber risk workshop in 2019 to provide an open forum for discussion of the "Cyber Risk Definition and Classification for Financial Risk Management" white paper (the paper was subsequently updated in 2020). The white paper aims to define and classify cyber risk for the purpose of financial risk management. For more information on the event see https://www.richmondfed.org/conferences_and_events/banking/2019/20191120_cyber_risk_workshop.

[21] The CERES Forum is an FS-ISAC group serving the needs of central banks, regulators, and supervisory entities. Information sharing among CERES Forum members occurs through a secure portal, coordinated conference calls, live events, and focused email distribution lists. For more information see https://www.fsisac.com/ceresforum.

[22] SWIFT established the SWIFT Information Sharing and Analysis Centre (SWIFT ISAC) as a global portal available to the SWIFT community. The ECRB Cyber Information and Intelligence Sharing Initiative is an information and intelligence sharing initiative among ECRB member volunteers.

enhances quantitative financial stability analysis and stress testing whereby financial institutions can leverage existing data consortia platforms.[23] If trusted networks between financial institutions are not already in place, central banks and supervisors can play a convening role to help promote such arrangements. Supervisory colleges can also be leveraged to share information and build trust.

33. **Establishing a globally agreed template for cybersecurity information sharing using a common taxonomy would be helpful.** While there is some convergence in definitions—such as what constitutes an incident that must be reported, what type of incident it was, and how to express the response—there is still a lack of commonality, which undermines effective sharing. A common taxonomy of cybersecurity information could support agreement and implementation of a standardized template for incident reporting. The development of a template could draw on the high-level categorization in this note (Table 1) and could make use of the FSB's cyber lexicon, which comprises a set of core terms related to cybersecurity in the financial sector. The template could be used as a one-stop-shop mechanism so that firms report incidents to their "home" or "lead" supervisor or authority, which would then coordinate with other supervisors and authorities. The template could also help ensure two-way information sharing so that not only do financial institutions report incidents to supervisors but information also flows in the other direction, alerting institutions to emerging issues, threats, or counterthreat measures as soon as possible. [24]

E. Deterring Cyber Threats

34. **Cyberattacks are a global phenomenon that presents significant challenges to law enforcement, especially at the international level.** The constant, rapid evolution of hacking technologies makes policing, prosecution, and sanction and asset recovery work difficult, even though there has been some success. Indeed, there are recent examples of successful cross-border investigations, such as Operation Taiex in March 2019, which led to the arrest of the organizer behind the Carbanak and Cobalt malware attacks on over 100 financial institutions worldwide. This operation included multiple law enforcement agencies and national authorities as well as private cybersecurity companies. Investigators found out that attackers were operating in at least 15 countries.

35. **International agreement on addressing cyberattacks is a politically sensitive topic.** The 2001 Budapest Convention is the only binding multilateral agreement aimed at combating cybercrime.[25] Offenses under the convention include (1) offenses against the confidentiality, integrity, and availability of computer data and systems; (2) computer-related offenses; (3) content-related offenses; and (4) criminal copyright infringement. In November 2019 a United Nations cybercrime resolution set up a drafting group to establish terms of reference for a new

[23] For example, Bouveret (2018) conducted analysis to estimate the potential loss to financial institutions from cyber threats using data obtained from the Operational Risk Exchange consortium.

[24] The evolving nature of the cyber threat landscape and risk management techniques calls for a simple, agreed process to update information sharing platforms and templates.

[25] An additional convention protocol was adopted in 2003.

global cybercrime treaty. The international constituency is divided, however, over fears of criminalizing ordinary online activities of individuals and organizations through cybercrime laws.[26]

36. **Cyberattacks generate a significant amount of illegal proceeds every year in advanced and developing economies alike.** Although cyberattacks may be committed for a range of motives (for example, political, competition, cyber war), many are profit-driven: some studies estimate that ransomware incidents alone generate some $1 billion in illegal proceeds every year (McGuire 2018). Developing economies face huge challenges as attackers exploit underinvestment in defenses and may even use these economies as testing grounds for new techniques. The proliferation of digital currencies that, when unregulated, provide anonymity and make it difficult, if not impossible, to trace the beneficiary owner or end receiver of funds makes it easier to generate and launder the proceeds of crime. In this context, the effective implementation of a comprehensive anti–money laundering and combating the financing of terrorism (AML/CFT) framework in all countries is crucial. In particular, requirements that private sector firms, such as banks, identify their customers, maintain relevant records, monitor transactions, and report suspicious transactions to the relevant authority are essential to prevent and combat cybercrime and the laundering of its proceeds. Sound AML/CFT frameworks also help with the recovery of the illegal proceeds of cybercrime.

37. **Cyberattacks should be made both expensive and risky through effective measures to seize and confiscate the proceeds of crime, as well as to identify and sanction bad actors.** Success in this respect is predicated on effective international cooperation; that is, information sharing and formal mutual legal assistance—otherwise cybercriminals simply shift operations to jurisdictions that do not cooperate effectively.

Box 2. International Organizations and Cyber Risk in the Financial Sector

The international standard-setting bodies—the Financial Stability Board (FSB), Basel Committee for Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI), and International Organization of Securities Commissions (IOSCO), among others—including the G7—have focused on developing a common language and approach to the regulation and supervision of cyber risk management in financial institutions. These efforts include the FSB Cyber Lexicon (FSB 2018) and Cyber Incident Response and Recovery toolkit (FSB 2020), the BCBS Cyber Resilience Range of Practices (BIS 2018), the CPMI/IOSCO principles for financial market infrastructures (CPSS 2012), and associated guidance on cyber resilience (BIS CPMI and IOSCO 2016) and form the foundation of global regulatory and supervisory standards to support consistency.

International financial institutions, including the World Bank, Inter-American Development Bank, and IMF, are focused on capacity development efforts. The IMF has concentrated on financial supervisors in low-income countries (Gaidosch and others 2019), incorporating cyber risk into financial sector surveillance and developing analytical tools to assist capacity development and surveillance and

[26] The UN special rapporteur on the rights to freedom of peaceful assembly and of association noted in May 2019 that "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world." (UN 2019, 2)

engagement in international policy discussions and regulatory initiatives to support member countries (Lipton 2020). An annual workshop for supervisors in low-income countries was launched in 2017, providing a forum for the sharing of experience by authorities at the forefront of addressing cyber risks. Workshops through the IMF's regional technical assistance centers are targeted to the particular needs of the region, and bilateral technical assistance has focused on improving national regulatory and supervisory frameworks. Initial efforts are working on the incorporation of cyber stress testing and cyber risk supervision in the Financial Sector Assessment Program (FSAP) and addressing analytical gaps.[1] A pilot exercise on the supervision of cyber risk as part of an FSAP is underway—with the first completed in Norway in 2020.[2]

The World Economic Forum and the Carnegie Endowment for International Peace, among other international groups, engage in public-private-sector work on cyber risk aimed at developing common standards and practices across the financial industry. Private sector and nonprofit organizations such as the Global Cyber Alliance, Cyber Defence Alliance, Financial Services Information Sharing and Analysis Center, and the Cyber Risk Institute promote information sharing and work with public sector entities to reduce inconsistencies and promote information sharing and cooperation between institutions.

[1] Examples of publications in this field include Goh and other (2020) and Bouveret (2018).

[2] See IMF (2020). Findings provided insight into avenues for improvement in Norway and allowed the FSAP to connect channels of contagion to an overall assessment of cyber risk. In addition, the 2019 Singapore FSAP assessed cyber risk as a key part of financial stability analysis and stress testing, investigated an institutional framework for cybersecurity, and proposed two (out of eight) key recommendations: one on developing a cyber network map and the other on enhancing the cyber resiliency of the central bank and the real-time gross settlement system.

AREAS FOR FUTURE WORK

38. **As we have seen, cyber risk is a global financial stability issue that demands a unified global effort.** Financial sector supervisors are working to improve and enhance regulatory frameworks and supervisory practices to address the risks from cybersecurity threats, but this work demands additional international focus to tackle gaps and inefficiencies and to ensure that emerging market and developing economies do not fall further behind. Our analysis suggests the following priority areas for further work:

Improving Cyber Risk Analysis and Integration into Financial Stability Analysis

39. Use of tools such as cyber mapping, stress testing, and improvements to the quantification of the potential impact of cyber incidents would enhance financial stability analysis, provide additional focus for the mitigation of cyber risks, and support the efficient allocation of resources. This work is being pioneered in central banks in many countries as well as by international financial institutions, including the IMF. Additional and sustained effort could produce significant gains in understanding the nature of the threat and appropriate avenues of response.

Greater Consistency in Regulatory Frameworks

40. **Financial supervisors could develop and promote greater consistency in the design and implementation of national cybersecurity regulatory frameworks.** Building on work by the FSB to introduce a cyber lexicon and effective practices in recovery and response, international standard setters across the financial sector could further improve the consistency of regulatory frameworks. This would support efforts to enhance information sharing, foster greater cooperation in response and recovery, and reduce the compliance burden on institutions. Outreach by international standard-setting bodies and others and capacity development by international financial institutions and other providers, as well as through public-private partnerships, could promote the broad use of international standards, building quality and consistency and establishing a global basis for information sharing and cooperation.

Enhancing Operational Resilience, Response, and Recovery

41. **Development and testing of national and cross-border response protocols would significantly improve the ability of authorities to successfully respond to cyber incidents.** Supervisors could require that financial institutions develop and test response and recovery procedures to ensure that firms remain operational even in the event of a major incident. National authorities could also work on developing clear and effective response protocols to potential crisis scenarios that may spill over to the entire financial sector and ensure that the financial system can continue to function. These would be tested regularly. Regional and international protocols for cross-border crisis management could be developed and regularly tested; for example, via national and international cyber crisis exercises.

Strengthening Information Sharing

42. **Addressing obstacles to the exchange of cybersecurity-related information is instrumental in promoting cybersecurity.** Obstacles to sharing should be identified and addressed cooperatively by financial institutions and supervisors. Working together, private and public sector actors could agree on what to share, when to share, how to share, and who to share with. Central banks, policymakers, and supervisors would actively encourage and support financial institutions' establishing and utilizing information sharing platforms that build trust. A commonly agreed on and internationally used template for information sharing built on a clear lexicon would also greatly reduce barriers to sharing.

Intensify the Defense against Cyberattacks

43. **Building strong domestic capabilities and enhanced cross-border coordination of investigation and enforcement against cyberattacks would strengthen deterrence.** Law enforcement agencies are working together across the globe, but this must be intensified and barriers to information sharing reduced. More effective implementation of sound domestic AML/CFT frameworks would strengthen the prevention of cybercrimes and the laundering of their proceeds, bolster law enforcement action when attacks do occur, provide channels for information sharing, facilitate the recovery of their proceeds, and ultimately reduce opportunities for cybercrimes.

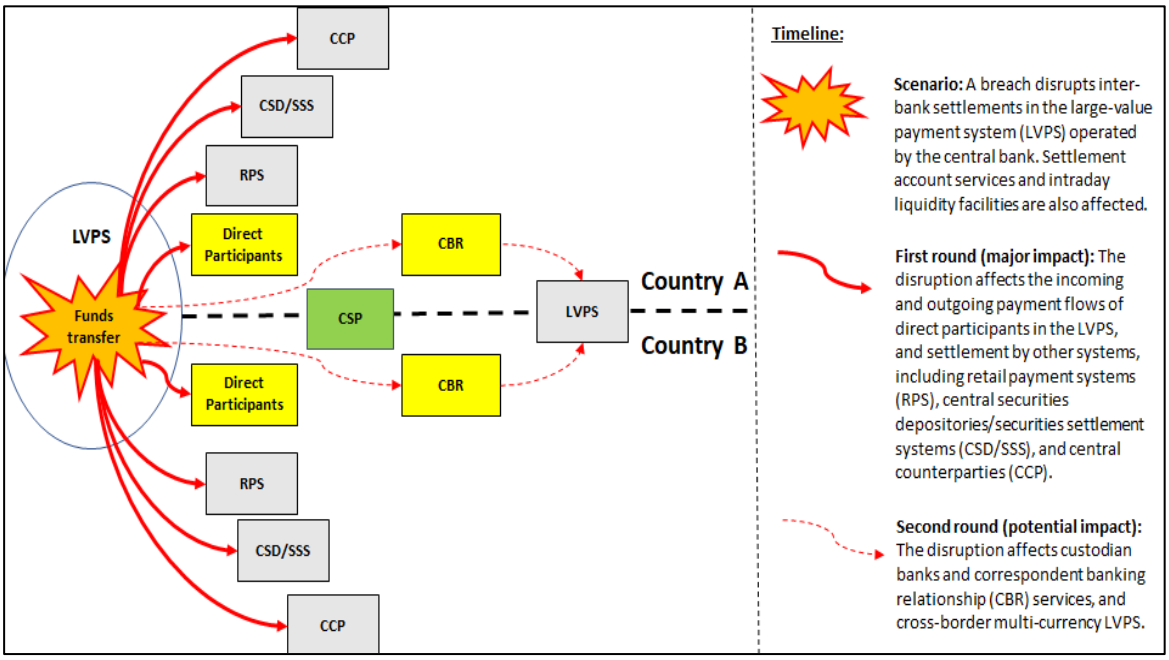
Capacity Development

44. **Building skills, resources, and operational capacity in all countries would have a global impact.** Cyber risk affects both advanced economies and low-income countries. Countries that fall behind in their ability to resist and respond to attacks will suffer disproportionately as other countries build stronger defenses. At the same time, attacks on countries strongly linked to the global financial system could spill over to others and endanger global financial stability. The international community has various programs in place to assist low-income countries with the development of technical skills and resources, but additional attention to capacity and global financial stability concerns would have benefits for the global community as a whole. International financial institutions, including the IMF, have an important role to play in supporting capacity building and delivering technical assistance to financial supervisors and central banks in developing economies to help them in their efforts to identify, measure, monitor, and address the risks to financial stability posed by cyber risks. This is imperative in an environment where the increasing digitalization of financial services delivery and the entry of many new providers may present new vulnerabilities.

APPENDIX I. FINANCIAL MARKET INFRASTRUCTURES (FMIs)

1. **Successful cyberattacks on FMIs[27] have the potential to transmit shocks to direct participants, other FMIs and their customers, and markets.** FMIs are key nodes in the financial system, often connected to most participants, responsible for a large volume of transactions daily and highly dependent on technology—making them a serious cyber risk concern. Possible scenarios related to successful attacks relate to confidentiality, service availability, and integrity.[28] A successful cyberattack on a systemically important payment system that processes large-value and time-critical transactions could transmit disruption to the entire financial system (across borders as well as domestically) with system, institutional, and environmental interdependencies (Figure 6).[29]

Figure 6. Cyberattack on Payment Systems and Possible Transmission Paths



Source: IMF staff.

2. **Cyberattacks against systemic banks can result in significant spillovers in the wholesale payment network.** According to a recent Federal Reserve System study (Eisenbach, Kovner, and Lee 2020) the impairment of any of the five most active US banks can affect as much as 38 percent of the network. Using a reverse stress test, the authors also found that interruptions

[27] FMIs refer to systemically important payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories. For further information see BIS and IOSCO (2016).

[28] BIS and IOSCO (2014).

[29] BIS (2008).

originating in some banks with less than $10 billion in assets may be sufficient to impair a significant proportion of the system.

3. **FMIs have been identified as critical infrastructures in some jurisdictions, requiring incident reporting and regulatory cooperation with the national cybersecurity agency.** FMIs are highly concentrated, connected, and systemic, and because of their unique role and characteristics, cyber threats to FMIs are increasingly considered a key risk to financial stability.

4. **Global efforts have aimed to further secure the core and peripheral parts of FMIs.** At the core, FMIs are normally required to have comprehensive information security policies, standards, practices, and controls as part of their operational risk-management framework.[30] FMI critical service providers (CSPs) such as IT and messaging services are also expected to meet the same standards on information security to ensure continuous and adequate performance.[31] Further guidance focuses on governance, risk management frameworks, settlement finality, operational risks, and FMI links.[32] At the periphery, enhancing endpoint security at banks, FMIs, and nonbank financial institutions is aimed at reducing the risk of wholesale payment fraud.[33]

5. **Some central banks have moved swiftly to strengthen the governance and cyber resilience of payment systems since the issuance of international guidance.** This includes establishing a cyber resiliency framework that comprises critical infrastructure such as central-bank-operated FMIs. Efforts to manage potential operational risks stemming from cyber risks have also been made, including expanding surveillance coverage, reinforcing protection capabilities, reducing time to recover, and developing cyber competencies. An approach developed by the European Central Bank to operationalize the CPMI-IOSCO guidance outlines five primary risk management categories and three overarching components that should be addressed.[34] The risk management categories include (1) governance, (2) identification, (3) protection, (4) detection, and (5) response and recovery. The overarching components cover (1) testing, (2) situational awareness, and (3) learning and evolving. Although the approach was designed in the European Union, it could also be used by other authorities and FMIs.

6. **Major efforts have also been made to improve CSP oversight and endpoint security.** For example, for SWIFT, authorities committed to considering legal reviews to investigate how moral suasion could be combined with a regulatory backstop, broaden membership of the SWIFT Oversight Forum, and improve information sharing on SWIFT oversight and assurance reports. Authorities have also set oversight priorities to monitor the effectiveness of the SWIFT Customer Security Program.[35]

[30] CPSS (2012).

[31] BIS and IOSCO (2014).

[32] BIS and IOSCO (2016).

[33] CPMI (2018).

[34] ECB (2018).

[35] NBB (2018) and NBB (2019).

APPENDIX II. OUTSOURCING AND THIRD-PARTY RISK

7. **Third-party risk management—including of cyber risk—is gaining importance as the number and scope of outsourced services continue to grow.** Financial institutions use a wide and increasing range of third-party providers, with some often servicing a large portion of the sector. Both the risks connected with the outsourcing itself and increasing concentration in a limited number of providers create challenges for regulators and supervisors because they are key contributors to financial stability risk. Cybersecurity failures in a major third-party provider could have a very serious impact on the sector as a whole. The use of third-party service providers is not new, so many jurisdictions have detailed policies in place. These are the key aspects typically covered:

A. Soundness of governance arrangements in the outsourcing institutions
B. Adequacy of pre-outsourcing risk analysis, due diligence, and contracting
C. Security of information and systems
D. Notification procedures for sub-outsourcing
E. Robustness of operational resilience arrangements
F. Right to access and audit the vendor (both by the outsourcing institutions and the supervisor)
G. Effectiveness of termination rights and exit strategies

8. **International bodies have made progress issuing guidance regarding third-party cyber risks, yet supervision in practice continues to prove challenging**. Examples are the G7 fundamental elements for third-party cyber risk management in the financial sector[36] and the Financial Stability Board publication "Third-Party Dependencies in Cloud Services—Considerations on Financial Stability Implications."[37] Critical vendors are typically not subject to the same depth of supervision as regulated financial institutions. While there is consensus that the responsibility for cybersecurity ultimately rests with the financial institution, supervisors have begun to discuss new ways of supervising these organizations. One model suggests that critical providers should be intensively supervised in the same way as utilities (such as energy)—that is, by a dedicated agency in charge of all critical infrastructure. Another model would entail the use of a trusted independent certification program, through which an agreed-on third party would set or attest to security standards in service providers. Yet another model calls for direct supervision by the financial sector supervisory agencies. This is an area calling for global cooperation since dominant service providers are global in nature.

[36] G7 (2016).

[37] FSB (2019b).

REFERENCES

Accenture. 2019. *Ninth Annual Cost of Cybercrime Study*, conducted by Ponemon Institute, Traverse City, MI. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50.

Adelmann, F., and T. Gaidosch. 2020. "Cybersecurity of Remote Work during the Pandemic." IMF Special Series on COVID-19, International Monetary Fund, Washington, DC. https://www.imf.org/~/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx.

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach. 2020. "Operational and Cyber Risks in the Financial Sector." Bank for International Settlements Working Paper 840, Basel. https://www.bis.org/publ/work840.pdf.

Bank for International Settlements (BIS). 2008. *The Interdependencies of Payment and Settlement Systems.* Basel. https://www.bis.org/cpmi/publ/d84.pdf.

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

_____ and International Organization of Securities Commissions (IOSCO). 2014. "Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers." Basel. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD468.pdf.

_____. 2016. "Guidance on Cyber Resilience for Financial Market Infrastructures." Basel. https://www.bis.org/cpmi/publ/d146.pdf.

Barrett, B. 2019. "The Catch-22 That Broke the Internet." *Wired*, June 7. https://www.wired.com/story/google-cloud-outage-catch-22/.

Boer, M., and J. Vasquez. 2017. "Cyber Security and Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System." Institute of International Finance, Washington, DC. https://www.iif.com/Portals/0/Files/IIF%20Cyber%20Financial%20Stability%20Paper%20Final%2009%2007%202017.pdf?ver=2019-02-19-150125-767.

Bouveret A. 2018. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." IMF Working Paper 18/143, International Monetary Fund, Washington, DC. https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx.

Carnegie Endowment for International Peace. 2017. "Timeline of Cyber Incidents Involving Financial Institutions." Washington, DC. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Committee on Payments and Market Infrastructures (CPMI). 2018. "Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security." Bank for International Settlements, Basel. https://www.bis.org/cpmi/publ/d178.pdf.

Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions (CPSS). 2012. "Principles for Financial Market Infrastructures." Bank for International Settlements, Basel. https://www.bis.org/cpmi/publ/d101a.pdf.

Doffman, Z. 2019. "Cybercrime: 25% of All Malware Targets Financial Services, Credit Card Fraud up 200%." *Forbes*, April 29. https://www.forbes.com/sites/zakdoffman/2019/04/29/new-cyber-report-25-of-all-malware-hits-financial-services-card-fraud-up-200/#6e6a2fff7a47.

Eisenbach, M., A. Kovner, and M. J. Lee. 2020. *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis,* Federal Reserve Bank of New York Staff Report 909. https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf.

European Central Bank (ECB). 2018. "Cyber Resilience Oversight Expectations for Financial Market Infrastructures. Frankfurt. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.

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

_____. 2019a. "Cyber Incident Response and Recovery." Progress report to the G20 finance ministers and central bank governors meeting in Fukuoka, Japan, June 8–9, 2019. https://www.fsb.org/wp-content/uploads/P280519-1.pdf.

_____. 2019b. "Third-party Dependencies in Cloud Services: Considerations on Financial Stability Implications. Basel. https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

_____. 2020. "Effective Practices for Cyber Incident Response and Recovery: Consultative Document." Basel. https://www.fsb.org/wp-content/uploads/P200420-1.pdf.

Gaidosch T., F. Adelmann, A. Morozova, and C. Wilson. 2019. "Cybersecurity Risk Supervision." IMF Departmental Paper 19/15, International Monetary Fund, Washington, DC. https://www.imf.org/~/media/Files/Publications/DP/2019/English/CRSEA.ashx.

Goh, J., K. Heedon, Z. H. Koh, J. W. Lim, C. W. Ng, G. Sher, and C. Yao. 2020. "Cyber Risk Surveillance: A Case Study of Singapore." IMF Working Paper 20/28, International Monetary Fund, Washington, DC. https://www.imf.org/~/media/Files/Publications/WP/2020/English/wpiea2020028-print-pdf.ashx.

Gray, A. 2017. "Credit Data Groups Face More Scrutiny after Equifax Hack." *Financial Times,* October 11. https://www.ft.com/content/52f4e97a-ad45-11e7-aab9-abaa44b1e130.

Group of Seven (G7). 2016, "G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector." Taormina, Italy. https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf.

Heijmans, R., and F. Wendt. 2020. "Measuring the Impact of a Failing Participant in Payment Systems." IMF Working Paper 20/81, International Monetary Fund, Washington, DC. https://www.imf.org/~/media/Files/Publications/WP/2020/English/wpiea2020081-print-pdf.ashx.

International Monetary Fund (IMF). 2020. *Norway: Financial Sector Assessment Program–Technical Note–Cybersecurity Risk Supervision and Oversight.* IMF Staff Country Report 2020/262, Washington, DC. https://www.imf.org/~/media/Files/Publications/CR/2020/English/1NOREA2020004.ashx.

(ISC)^2. 2019. *Cybersecurity Workforce Study.* Clearwater, FL. https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482.

LaVito, A. 2017. "Equifax Security and Information Executives to Retire." CNBC report, September 15. https://www.cnbc.com/2017/09/15/equifax-security-and-information-executives-to-retire-dj-reports.html.

Lipton, D. 2020. "Cybersecurity Threats Call for a Global Response." Blog. International Monetary Fund, January 13. https://blogs.imf.org/2020/01/13/cybersecurity-threats-call-for-a-global-response/.

McGuire, M. 2018. *Into the Web of Profit.* Cupertino, CA: Bromium. https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf.

National Bank of Belgium (NBB). 2018. "The Financial Market Infrastructures and Payment Services Report." Brussels. https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2018/fmi-report2018.pdf.

_____. 2019. "The Financial Market Infrastructures and Payment Services Report." Brussels. https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2019/fmi-report2019.pdf.

Office of Financial Research. 2017. "Cybersecurity and Financial Stability: Risks and Resilience." Washington, DC. https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf.

United Nations Human Rights Council (UN). 2019. "Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association." New York. https://www.ohchr.org/Documents/Issues/FAssociation/A_HRC_41_41_EN.docx.

World Bank (WB). 2019. "Cyber Resilience for Financial Market Infrastructures." Washington, DC. http://pubdocs.worldbank.org/en/189821576699037673/FIGI-ECB-OperationalCyber-FinalWeb-12-13.pdf.

Additional Reading

Almansi, A., Y. C. Lee, and J. Lincoln. 2017. "Financial Sector's Cybersecurity: A Regulatory Digest." World Bank, Washington, DC. http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf.

Carriere-Swallow, Y., and V. Haksar. 2019. "The Economics and Implications of Data: An Integrated Perspective." IMF Departmental Paper 19/16, International Monetary Fund, Washington, DC. https://www.imf.org/~/media/Files/Publications/DP/2019/English/TEIDEA.ashx.

Curti F., J. Gerlach, S. Kazinnik, M. Lee, and A. Mihov. 2020. "Cyber Risk Definition and Classification for Financial Risk Management." Federal Reserve Bank of Richmond, Richmond, VA. https://www.richmondfed.org/-/media/richmondfedorg/conferences_and_events/banking/2019/cyber_risk_classification_white_paper.pdf

Kashyap, A., and A. Wetherilt. 2018. "Some Principles for Regulating Cyber Risk." *AEA Papers and Proceedings* 109:484–87.

Kopp E., L. Kaffenberger, and C. Wilson. 2017. "Cyber Risk, Market Failures, and Financial Stability." IMF Working Paper 17/185, International Monetary Fund, Washington, DC. https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx.