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.