

SEPTEMBER 2019

Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #4

Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment

Lincoln Kaffenberger and Emanuel Kopp

Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment

Lincoln Kaffenberger and Emanuel Kopp

For your convenience, this document contains hyperlinked source notes indicated by [teal-colored text](#).

© 2019 Carnegie Endowment for International Peace. All rights reserved.

The views expressed in this book are those of the authors and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

Carnegie does not take institutional positions on public policy issues: the views represented herein are the authors' own and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace. Please direct inquiries to:

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

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

+ CONTENTS

Cybersecurity and the Financial System	v
About the Authors	vi
Abstract	1
Introduction	1
Properties of Cyber Risk	2
Scenarios	8
Assessing Systemic Cyber Risk on the National Level	13
Ways to Mitigate Risk	19
Conclusion	21
Notes	23

Cybersecurity and the Financial System

Carnegie’s working paper series “Cybersecurity and the Financial System” is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie’s FinCyber newsletter providing you with a curated regular update on latest developments regarding cybersecurity and the financial system: <https://carnegieendowment.org/subscribe/fincyber>.

If you would like to learn more about this paper series and Carnegie’s work in this area, please contact Tim Maurer, co-director of the Cyber Policy Initiative, at tmaurer@ceip.org.

Papers in this Series:

- “Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment” Lincoln Kaffenberger and Emanuel Kopp, September 2019
- “The Cyber Threat Landscape: Confronting Challenges to the Financial System” Adrian Nish and Saher Naumaan, March 2019
- “Protecting Financial Institutions Against Cyber Threats: A National Security Issue” Erica D. Borghard, September 2018
- “Toward a Global Norm Against Manipulating the Integrity of Financial Data” Tim Maurer, Ariel (Eli) Levite, and George Perkovich, March 2017

About the Authors

Lincoln Kaffenberger works as an information security professional in the financial sector. He is also a co-author of the IMF's seminal paper on cyber risk ("Cyber Risk, Market Failures, and Financial Stability," 2017). He has over a decade of experience helping organizations understand the threats they face and make informed, risk-based decisions.

Emanuel Kopp is a senior economist with the International Monetary Fund. His research interests include macrofinancial risk, financial stability and regulation, investment, and macroeconomic forecasting. Before joining IMF, Kopp was an assistant professor of finance and a central banker.

Abstract

Cyber risk has become a key issue for stakeholders in the financial system. But its properties are still not precisely characterized and well understood. To help develop a better understanding, we discuss the properties of cyber risk and categorize various cyber risk scenarios. Furthermore, we present a conceptual framework for assessing systemic cyber risk to individual countries. This involves analyzing cyber risk exposures, assessing cybersecurity and preparedness capabilities, and identifying buffers available to absorb cyber risk–induced shocks.

Introduction

Internet usage is globally expanding at a rapid pace. According to the International Telecommunications Union (ITU), 1.5 billion new users accessed the internet between 2010 and 2016.¹ Although internet access fosters digital, social, and financial inclusion, the ever-expanding digitalization of life increasingly provides opportunities for adversaries. These opportunities range from criminals conducting financial fraud and information theft to sophisticated hackers conducting disruptive and even destructive cyber attacks.

Assessing and managing systemic cyber risk remains challenging. The financial system has so far weathered larger-scale cyber attacks, but some argue that the system has not been tested for a truly systemic event.² As the connection between cyberspace and the real economy intensifies—amid widely expected further increases in interdependency, interconnectivity, and complexity—the probability that an external shock will affect the financial system and become a systemic event increases.³ Further, the inherent lack of transparency into highly integrated operations and interdependencies complicates an ex-ante assessment and quantification of systemic cyber risk. Data are scarce, and only rarely is cyber risk measured in terms of economic costs. Finally, modeling techniques for both idiosyncratic and systemic cyber risk are less advanced than they are for other insurable risks, and it appears that more work needs to be done to put these on a solid footing.

Although companies have become increasingly aware of the need to prevent cyber breaches, the concept of systemic cyber risk remains largely abstract. Some see cyber risk as simple operational risk—a cost component of doing business in an interconnected world—and do not factor systemic cyber risk into their risk calculus. Others float Armageddon-style scenarios about a massive cyber attack that would bring our modern financial and social system to its knees, though rarely in a way that is useful for risk management. In an attempt to increase the understanding of how cyber risk can potentially manifest, we present a systematization of potential cyber risk events, ranging from limited, idiosyncratic scenarios to widespread, systemic ones.

This paper aims to help strengthen the understanding and increase the awareness of systemic cyber risk among stakeholders in the financial system. First, we discuss the properties of cyber risk, including risk aggregation and the different dimensions of cyber risk. To make cyber risk less abstract, we outline various scenarios, ranging from firm-specific operational risks to upstream infrastructure disruptions and external shocks. Reading about possible scenarios can help policymakers develop a more comprehensive view of how cyber risk can manifest. Second, we outline a framework for assessing systemic cyber risk on the country level, based on cyber risk exposures, cybersecurity preparedness, and resilience to shocks.

Properties of Cyber Risk

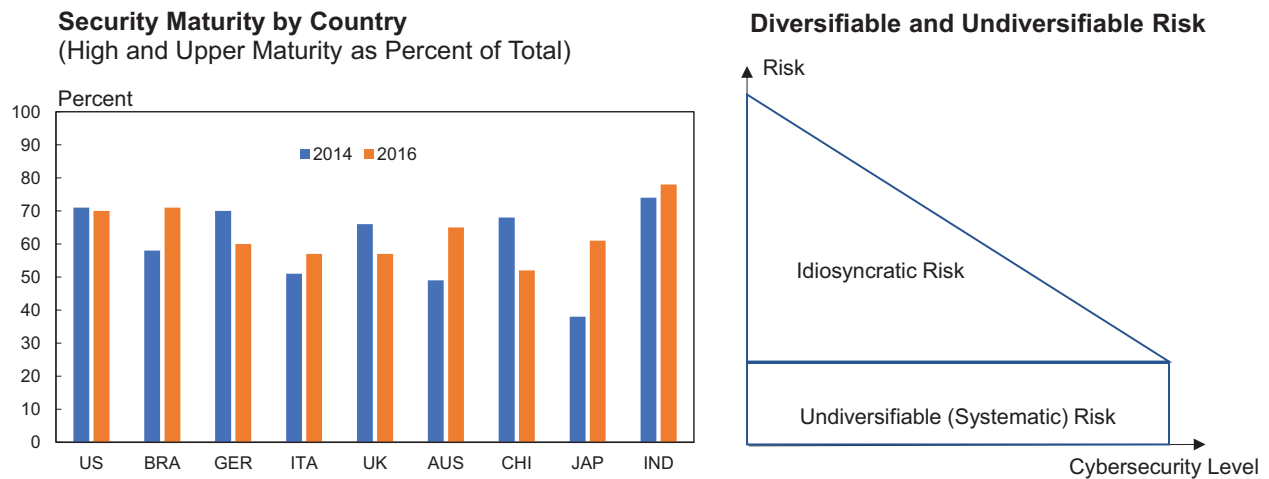
Complexity and Risk Aggregation

Especially over the past fifteen years, the number of users and devices connected to the internet has skyrocketed. This trend has been driven predominantly by the widespread use of mobile phones throughout the world. According to Cisco, worldwide, the number of internet-connected devices increased from 500 million in 2003 to 12.5 billion in 2010, equivalent to an average increase of 35 percent a year.⁴ According to estimates, the number of Internet of Things (IoT) devices—electronic items that can connect to the internet or local networks, including smart TVs and refrigerators—increased from approximately 20 billion in 2017 to 31 billion in 2018.⁵ As with other technical devices and software, many of these IoT devices are assumed (or known) to have technological vulnerabilities that are often left unaddressed by both the manufacturers and the owners.

Software flaws expose users to cybersecurity risk. Many software problems only become known when products have been used by a sufficiently large network of people. With increasing software maturity (Figure 1, left chart), products typically become safer. But there are also economic incentives for software vendors to roll out products sooner than the competition, and to address security issues on the fly.⁶ Software vendors may decide to invest less in security so that their services can compete at lower prices.⁷ The use of third-party software or networks necessarily means being exposed to undiversifiable risk (that is, the portion of cyber risk that cannot be diversified away irrespective of individual cyber hygiene; Figure 1, right chart). No matter how careful network participants are (that is, how well they manage their idiosyncratic risk), the mere use of third-party software or the internet means exposure to undiversifiable risk.⁸ Information asymmetries and misaligned incentives can cause chronic underinvestment in cybersecurity, creating negative externalities that are borne by other network participants.

Hackers exploit security weaknesses and compromise vulnerable devices to conduct cyber attacks. Threat modeling can help overcome the lack of reliable cyber risk data. Information about

FIGURE 1
Security Maturity by Country; Cybersecurity and Risk



SOURCE: CISCO (2017), Figure 67.

the type of hacker responsible for a cyber attack helps narrow the range of relevant scenarios: motives and capabilities to perform attacks vary across different types of cyber threat actors (Table 1).⁹






- *Criminals, hacktivists, and insiders range from unsophisticated to sophisticated.* Whereas some criminal groups demonstrate a high degree of sophistication, a large cyber event that damages the financial sector does not align with their incentives to make money at minimum risk. One conceivable systemic scenario is where the volume of successful cyber crime events reaches such a high level that it disrupts consumer confidence in the financial sector. In effect, the cyber criminals would be like leeches that inadvertently kill their host.
- *Proxy actors typically conduct offensive cyber operations on behalf of a beneficiary, who may be a competitor, national government, or group of individuals.* Although proxy actors' activities are mostly considered espionage, they also conduct other types of cyber attacks, including those that are logically and physically destructive.
- *Nation-states engage in long-term espionage and offensive cyber operations that support geopolitical and strategic policy objectives.* Many nations have increased their capabilities to conduct cyber attacks, including military-style, destructive cyber attacks. In 2018, the U.S. Intelligence Community identified more than thirty countries with military-grade destructive cyber attack capability.¹⁰

The financial sector and the economy in general could be potential targets in the event of war.

The increasingly aggressive posture of nations' militaries in cyberspace,¹¹ a shift toward hybrid warfare¹² or unrestricted warfare¹³ in the past two decades, and recent changes in the tone of military leaders¹⁴ highlight the fact that the economy and the financial sector in particular are increasingly

TABLE 1

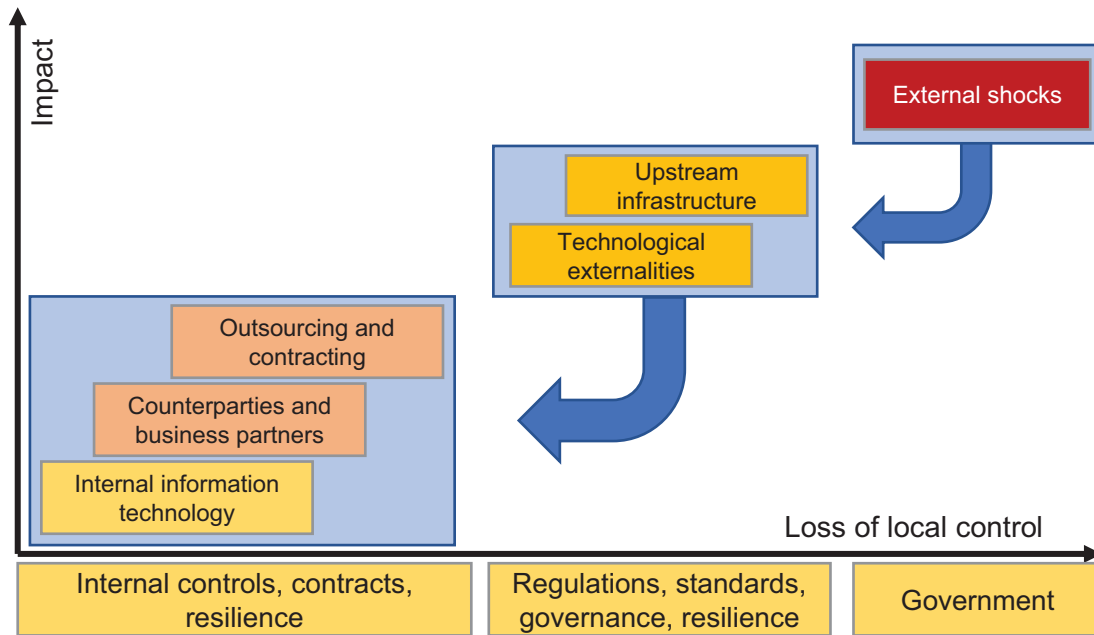
Threat Actors: Motives, Impact, and Relevance

	Category	Actions	Real/Possible Impact	Frequency
	Nation-states	<i>Monitor other nations' economies for espionage; conduct cyber-attacks in rare cases.</i>	Loss of trust once breach is discovered; disruption to the financial sector.	Espionage—common Destruction—very rare
	Proxy Organizations	<i>Steal information for espionage; possibly conduct destructive attacks.</i>	Loss of trust once breach is discovered; disruption to the financial sector.	Espionage—common Destruction—very rare
	Cybercrime	<i>Steal money from financial sector entities; at times stealing large sums.</i>	Affects organizations' profits; loss of trust if breach is publicized but org was silent	Theft—very common
	Hacktivist	<i>Disrupt financial sector operations; attack the brand of individual institutions; data release individual/institutions.</i>	Damaged reputation; loss of trust	Moderately common
	Insider	<i>Steal money; get revenge through destruction or data release.</i>	Affects organizations' profits; damaged reputation	Moderately rare

considered potential targets. Attacks on a nation's economy could involve the destruction, degradation, or disruption of either a specific company or set of companies (for example, important banks) or important functions, like transaction clearing and settlement.

Cyber risk has long been viewed mainly as an internal information technology (IT) security issue. Cyber risk was seen as an idiosyncratic operational risk of doing business through networks (for example, the internet) and of using software. Over time, this perspective has evolved to include operational risks linked to the firm's immediate business partners, including counterparties and third parties. Internal risk management processes and controls have extended to cover firms and customers that are immediately related to the firm's business. Indeed, the true aggregation of risks goes well beyond individual institutions (Figure 2). Risks stemming from upstream infrastructure (for example, electricity, telecommunications, financial market infrastructures) or technological externalities (for example, the entry of disruptive new technologies) are outside the control of individual firms. Despite the (typically expansive) contracting arrangements, it remains challenging to monitor cyber risk exposures even of close business partners. Risks can also arise from unanticipated external shocks, like natural disasters or armed conflict, that require government intervention.

FIGURE 2
Impact, Shock Transmission, and Control



SOURCES: Atlantic Council, *Beyond Data Breaches: Global Interconnections of Cyber Risk*, Zurich Insurance Group, Risk Nexus, April 2014; Kopp, Kaffenberger, and Wilson, “Cyber Risk, Market Failures, and Financial Stability,” International Monetary Fund Working Paper WP/17/185, 2017; and authors’ research.

Significant uncertainty surrounds the potential financial impact of cyber events. Whereas there are relatively well understood direct costs related to cyber incidents (including, for example, the cost of forensic investigation, legal assistance, customer notification, postbreach customer security, and credit protection), indirect costs are less visible, longer term, and more difficult to quantify ex-ante.¹⁵ These include negative effects on brand name and customer relationships (reputational risk), depreciation of intellectual property value, and higher ongoing operational expenses and risk costs. Globally, cyber losses have been estimated at \$250 billion to \$1 trillion a year.¹⁶

Systemic Risk

Cyber risk not only affects individual financial institutions but has an important systemic dimension. The World Economic Forum (WEF) defines systemic cyber risk as “the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security.”¹⁷ Whereas cyber risk as an operational risk has been

on risk managers' radar screens for a while now, risk management in financial institutions has until recently concentrated on the individual firm, largely disregarding the systemic nature of cyber risk arising from the dependence on complex infrastructure or from disruptions of critical information systems. The predominance of cyber risk assessment on the level of individual institutions has grown but increasingly signals a relatively narrow view that often disregards, or inadequately includes, the systemic dimension of cyber risk to systems and networks.

Assessing systemic cyber risk is hampered by structural challenges. These arise from inexperience with large cyber events; uncertainty around how shocks would transmit; the lack of comprehensive and cohesive data about events; and uncertainties around long-term impacts of cyber breaches. Complex risk aggregation in the cyber domain has been particularly challenging for estimating the cost of past and future cyber events.¹⁸ Further, incentives are skewed toward the victim institution not revealing the scale or nature of cyber attacks.¹⁹

Systemic risk arises from risk concentration, risk correlation, and shock amplification. The Office of Financial Research refers to lack of substitutability, loss of confidence, and loss of data integrity as channels through which cybersecurity events can threaten financial stability.²⁰ Columbia School of International and Public Affairs discusses “lack of financial substitutability, lack of IT substitutability, loss of confidence, data integrity, and interconnectedness.”²¹ For example, certain systems, including central clearing platforms (CCPs) and transfer systems like SWIFT, are key hubs within the financial system.²² Although these provide standardization and secure global financial services, they also create concentration risk due to low external redundancy.²³ Their services cannot be easily replaced by other institutions, because although financial infrastructure systems are technically highly redundant, their functions are not. Downtimes or defaults can impact payment, clearing, and settlement of financial transactions, with negative externalities, exposing financial institutions, markets, and participants to unexpected shocks. Interlinkages that span the financial system allow idiosyncratic shocks to spread widely and potentially become systemic.

The main sources of systemic cyber risk are exposures to risk concentration via lack of substitutability; loss of confidence and risk correlation; and complex interconnections that amplify effects.

- *Risk concentration and lack of substitutability:* Risk is concentrated in a number of financial market infrastructures and systemically important financial institutions. But systemic risk can also arise from technical and IT concentration, including from operating systems and programs, cloud servers, and electronic network hubs. These “single points of failure” are especially important for the proper functioning of the financial system, as disruptions immediately affect large parts of the financial economy.

- *Loss of confidence and risk correlation:* Idiosyncratic cyber shocks can cause a loss of confidence that triggers funding liquidity risks, which can turn into market liquidity shocks, market risk, and, ultimately, solvency risk. An institution's inability to meet payment or settlement obligations can cause a name crisis, with adverse effects on funding liquidity. The default of institutions hit by cyber risk causes counterparty credit risk to manifest. Other institutions that counted on the availability of these liquidity flows may also be threatened by liquidity cascades. Liquidity shortages in turn may require institutions to sell assets in fire sales (increasing market liquidity risk), which would then affect asset valuation and spread to all kinds of market participants invested in or trading that asset or asset class. Over time, liquidity risk–induced losses eat into firms' capital, potentially causing a solvency crisis.
- *Complex interconnectedness that amplifies contagion:* Close, direct connections through inter-bank and transfer markets allow shocks to spread throughout the system. Amid increasing digitalization, the networks that build our financial systems have experienced a dramatic increase in the number of interconnections and the level of complexity. Shocks in one part of the system may affect other, perhaps remote areas of the financial system through indirect interconnections or the emergence of previously unknown dynamics with unanticipated feedback.

BOX 1

The NotPetya Datawiping Worm: A Glimpse at Systemic Cyber Risk

The closest example to a systemic cyber risk event—the NotPetya attack—started in Ukraine in late June 2017. A self-replicating computer virus used an exposed nation-state-grade technology exploit as well as several other advanced techniques to infect thousands of computers.²⁴ The total costs from NotPetya are estimated to have ranged between \$2 billion and \$10 billion.²⁵ The attack took some networks down for several weeks.²⁶

The event revealed some possible characteristics of a future systemic cyber event: fast propagation, causing a high number of victims in a short period of time; intended logical or physical destruction of a system that leads to disruption of an organization's mission or business operations; and collateral damage outside the intended victim. Cyber insurance may not cover such events as they could fall into the “war clause” exemption.²⁷

Scenarios

Scale and Timing

For a cyber event to leave a significant impact on the economy, many experts believe that it would have to be large. Depending on the scale of the event, the number of scenarios, and the timing of the scenarios, an initially operational event could grow into a systemic event. Figure 3 describes several possible ways this could play out. A systemic cyber event could, for instance, be caused by a series of seemingly small or idiosyncratic cyber events that have cascading effects due to previously unknown linkages and dependencies among affected organizations.

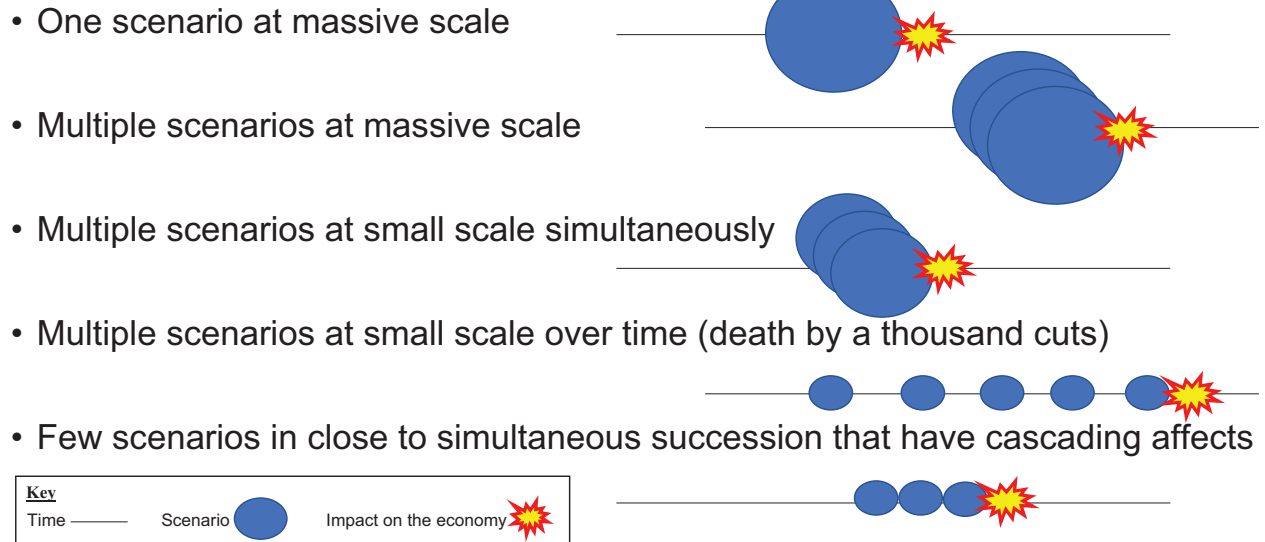
Timing will play an important role in the materialization of a systemic cyber event. Timing affects organizations' ability to respond to events, the resources they have available to mitigate financial loss, and their ability to manage damage to their reputation. Timing at the system or national level affects when certain financial sector functions are more used (that is, more critical), hence increasing the impact of their loss or disruption. Because timing and triggers of financial crises are hard to predict, analysis of financial system stability focuses on identifying vulnerabilities in the system and building buffers to increase resilience to shocks.²⁸ At certain times, the system is less able to do so, and should a shock occur at that moment it could trigger a significant impact on the economy. For example, publicly traded firms are more at risk around quarterly filing time and around announcements of merger or acquisition or payout policy. CCPs, which concentrate the risk of members' settlement failures into themselves, are more at risk around the time of settlement, when the accumulated debt obligations are particularly high and the risk of having to tap into liquid assets and liquidity lines is generally elevated.²⁹

An analysis of hypothetical adverse scenarios can help firms and policymakers identify and implement the most effective risk-mitigating factors. The scenario-design process requires identifying potential sources of risk, describing how the risk would affect the firm, and describing how shocks would transfer through the system. Such thought experiments are forward-looking, can integrate the effect of future technologies, are dynamic (as shocks transmit through systems), and to some extent are probabilistic. Scenario analysis can help institutions understand potential risks, how they may transmit, where investments need to be made, and how best to respond when systems are breached.

Systematization of Cyber Risk Scenarios

The starting point is a thorough risk assessment. Where does the risk originate: within the current realm of operational risk (that is, an event directly affecting the organization or coming from its third parties), from the organization's upstream infrastructure, or from an external shock? One of the

FIGURE 3
Scale Considerations



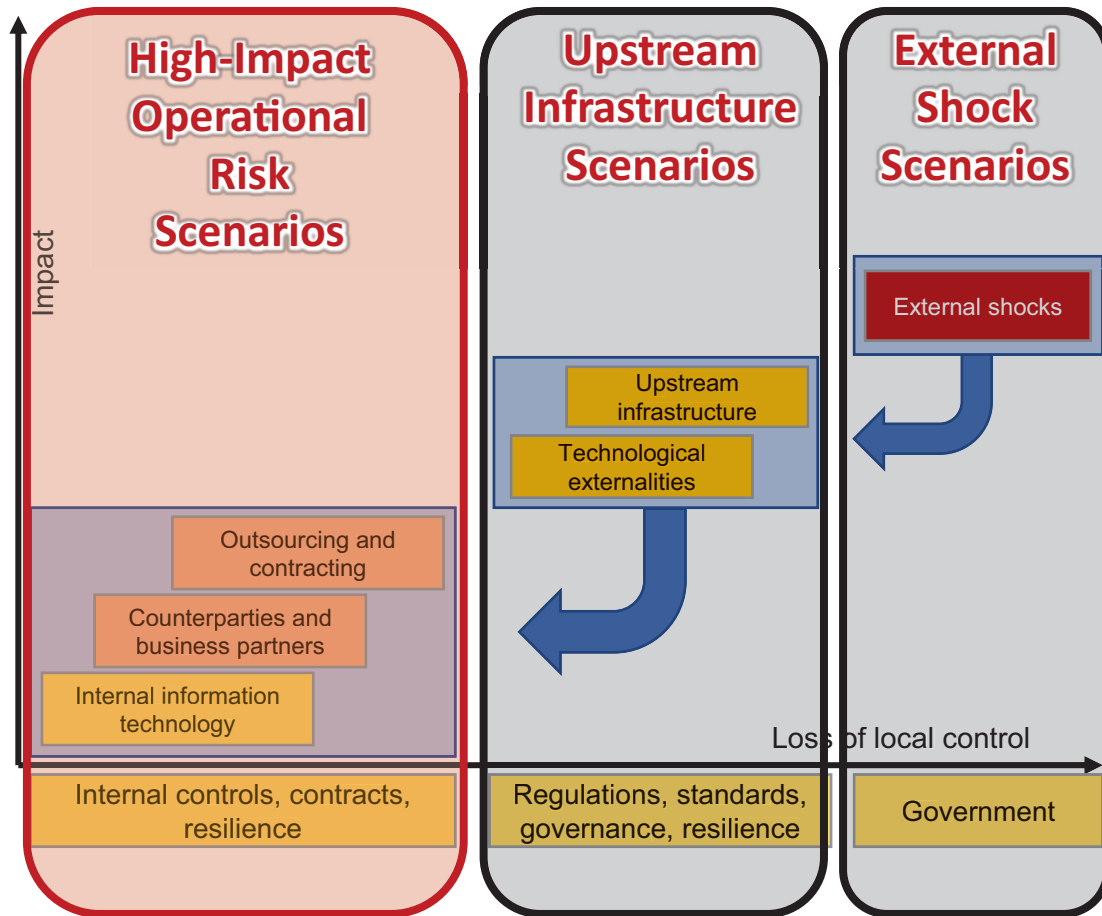
big advantages of scenario analysis is that not only past events but also potential future events can be simulated. For a quickly evolving risk factor like cyber, past events are not necessarily good indicators of future patterns. Below, we provide a list of actual and prospective future scenarios from which analysts can inform their own scenario selection. Using a classification first proposed by the Atlantic Council, we discuss (more traditional) high-impact operational risk scenarios, upstream infrastructure scenarios, and external shock scenarios (Figure 4).

High-Impact Operational Risk Scenarios

Operational risk is the risk of loss resulting from failed or inadequate internal processes, people, and systems, or from external events that affect internal IT.

- **Hypothetical Scenario #1—Locking Malware or Ransomware Attack on a financial institution:** A large bank becomes the victim of a ransomware attack that causes the majority of the bank’s computers to effectively become unusable, resulting in operational disruption and client service disruption. The Shmoon virus, for instance, infected some 35,000 computers at the energy company Saudi Aramco.³⁰ The attack destroyed 85 percent of the company’s hardware and for ten days made business operations impossible.³¹ Another well-known example of a ransomware attack is WannaCry, a ransom cryptoworm that affected more than 200,000 computers across more than 150 countries.

FIGURE 4
Key Cyber Risk Scenario Types



SOURCE: Atlantic Council, *Beyond Data Breaches*; extended by authors.

- **Hypothetical Scenario #2—Large Wire Transfer Fraud:** A financial institution experiences a significant monetary loss from a fraudulent transfer induced by a cyber attack. Criminals steal funds with the help of an insider who facilitates placing malware within the environment. They conduct successful internal-social engineering to orchestrate large transfers from the institution to accounts controlled by the criminals.
- **Hypothetical Scenario #3—Data Breach and Targeted Information Leak:** A ratings agency is compromised, and the attackers steal sensitive data about rated companies and other financial institutions as well as the agency’s emails and other internal documents. The attackers publicly release incriminating emails, documents, and select company information

after a failed extortion attempt. The incriminating emails call into question the authenticity of the agency's ratings with accusations of quid pro quo deals for good ratings by rated organizations.

- **Hypothetical Scenario #4—Placing Malware in Trading Systems:** Malware induces abnormally large trading volumes that affect price discovery. A large asset-management firm is compromised, and the malware causes several simultaneous, high-dollar trades of a certain commodity. The trades destabilize the market, causing large fluctuations in the commodity price. Also, a cyber attack on automated trading causes the malfunction of algorithmic programs by taking advantage of trading complexity and capacity, disrupting markets and increasing the risk of market misconduct such as unsolicited information leakage and possible market manipulation of “dark pools” (private exchanges for trading securities). A cyber attack can also bring trading to a halt; trading stops at a stock exchange after it is suspected that wild movements in stock prices of a few firms were the result of the exchange's main trading platform being compromised.
- **Hypothetical Scenario #5—A large-scale cyber attack on a global messaging network for financial transactions:**³² A global messaging network for financial transactions suffered a large-scale, persistent series of cyber attacks over a period of four weeks. It never became known what exactly was the nature of the events that forced the network to discontinue the service and shut down. Many anonymous sources within various financial institutions reported issues with their attempts to send messages over the network; the recipients never received the messages or received an altered message.
- **Hypothetical Scenario #6—Simultaneous Cyber Attacks on Systemically Important Institutions:** A number of major attacks on critical core infrastructures occur at the same time. The attacks include a systemically important bank losing millions in a heist, followed by a systemically important insurer suffering a large ransomware event at the same time that a major regulator suffers a public data breach. Though there is no evidence that conclusively links the three separate attacks, the timing is seen as “no coincidence” by pundits and causes major negative shocks to the country's and region's financial sector.

Upstream Infrastructure Scenarios

- **Hypothetical Scenario #1—Disruptions to Central Clearing:** A CCP is the victim of coordinated cyber attacks that disrupt its ability to perform its functions, resulting in inability to clear trades. The attack campaign continues for multiple months, causing several of the CCP's clients to find alternative means for reliable clearing and settling.

- **Hypothetical Scenario #2—Attack Disrupts Payment-Processing Gateways:** A cyber attack causes intermittent disruptions of a retail payments system over the period of a week, affecting tens of thousands of companies and their customers throughout several countries.
- **Hypothetical Scenario #3—Massive Malware Infection:** Millions of network routers worldwide begin malfunctioning simultaneously due to malware that was installed surreptitiously at the factory. Large portions of internet traffic are disrupted. Along with disruption throughout other sectors, payment processing is disrupted for multiple days as the vendor races to solve the problem without success. The only timely solution is for companies to buy routers from a different vendor that is unaffected by the malware. Demand spikes and shortages follow, resulting in a delayed recovery and material impact to the economy.
- **Hypothetical Scenario #4—Cloud Provider Fails:**³³ A large cloud provider fails suddenly for unforeseen reasons. Companies reliant on the provider can no longer operate. Firms depending on just-in-time products lack supplies, affecting companies that depend on them. Large parts of the economy suffer, with effects being felt in other countries as well. Consequently, many businesses lose trust in the internet as a way to do business and demand that suppliers and third parties establish redundancy.
- **Hypothetical Scenario #5—Utilities Disruption Causes Knock-On Effects:** Disruptions of upstream infrastructures can have knock-on effects on the financial sector and economy. The financial sector—along with all other critical infrastructure sectors—depends on electricity, functioning communications that telecoms provide, and properly functioning technology.³⁴ Prolonged disruptions to the functioning of these dependencies will impact the financial sector’s ability to deliver its services and function.

External Shock and Other Scenarios

- **Hypothetical Scenario #1—Sanctions Retaliation via Cyber Attack:** In response to sanctions and as part of a broader national effort, the sanctioned country directly targets financial sector institutions within the sanctioning countries with a combination of different cyber attacks. Though larger banks are primarily responsible for the sanctions, the sanctioned country determines that it can have a bigger impact by targeting many small and medium banks because they are less well defended. The attacks include disruptive attacks that affect institutions’ connectivity; multiple data breaches and leaks of sensitive data from multiple small and medium banks; public claims that releases of data from larger institutions will follow; and multiple thefts from small and medium banks. Due to the prolonged nature of the attacks, public confidence and trust in the financial sector is significantly

damaged, resulting in several runs on smaller banks and the risk of liquidity shocks spreading through the sector.

- **Hypothetical Scenario #2—Armed Conflict:** A country engages in armed conflict with a rival country. As part of the opening stages of the conflict, one country conducts targeted attacks on its rival’s governmental cloud service providers, telecommunications infrastructure, and energy distribution centers. The intent is to blind and delay its rival’s military response so that a narrow and limited objective is achieved before the rival can mount a coordinated response. The attacks have secondary effects on the rival’s financial sector and on the financial sector’s third-party service providers. The outages cause disruptions with payments, claims, disbursement, trading, and clearing for multiple weeks.

Assessing Systemic Cyber Risk on the National Level

Each country has a different susceptibility to systemic cyber risk. Assessing systemic cyber risk is challenging and made more difficult by the fact that each country has a different level of susceptibility to a major cyber event causing a shock to the financial system. If risk managers understand the differences by country, they are better equipped to help assess the risk of a systemic cyber event materializing in a given country.

This section outlines a conceptual framework for assessing systemic cyber risk on the national level (Figure 5). The first step is an assessment of a country’s risk exposure. We consider the following in our assessment of current and potential future cyber threats faced by financial and government institutions: (1) the country’s dependence on technology, and (2) its degree of connectivity. For a country’s financial system, the exposure to systemic cyber risk depends on the adoption and usage of electronic banking, payments, and mobile money systems. The next step is an assessment of cybersecurity and the country’s preparedness to manage cyber risk as a first line of defense against such risk. Finally, the country’s resilience to shocks to the financial sector depends on the size of available buffers to absorb a cyber attack’s effects. Buffers can include the institutions’ reserves, stock and flow of liquid assets, public backstops (if available), and interconnectivity within the financial system.

FIGURE 5
Overview of Assessment Approach



Analysts can tailor the conceptual framework to their case by introducing *alternative or additional* measures for identifying risk exposure, the level of cybersecurity, and the types and respective sizes of available buffers. The idea is to tailor the conceptual framework to one's case: types of financial institutions and infrastructures are differently exposed to risk; technological dependence is time-varying; cybersecurity levels tend to increase over time; and the financial system's ability to absorb shock is subject to change over time. These properties require a flexible, tailored approach. Next, we define in more detail the components of the methodology and provide for illustrative purposes a relatively simple specification of the framework.

Cyber Risk Exposure

Cyber Threat Level

The cyber threat assessment is typically a compilation of publicly available quantitative and qualitative information. In such assessments, analysts study historical patterns of cyber attacks against a country and its financial sector using a myriad of sources. The analysis often indicates which threat actors have been attacking a country's financial institutions and thus the potential magnitude of the threat. For instance, large cyber events are more likely to be caused by nation-states or their proxies. Countries more exposed to such perpetrators have a higher likelihood of experiencing a large systemic event. One way to bring this into a quantitative framework is to assign numeric values across the threat spectrum (from low to high). Relative comparisons are helped by transforming values into z-scores. Table 2 describes assessment criteria for the cyber threat assessment.

Technology Dependence

The increased usage of technology and the quick adoption of new technologies increasingly provide opportunities for adversaries. In cyber risk management, the technological exposure to cyber risk is summarized by an attack surface, which is a collection of vulnerabilities that can be exploited to carry out a cyber attack, including unauthorized accessibility. Access vulnerability risks increase with rising connectivity, which means more exposure to systemic cyber risk.

For this example (in Figure 6), we use the share of the population that utilizes digital payments, transformed into z-scores, as a simple gauge of both online activity and financial sector dependence on technology.³⁵ This variable is highly correlated with other measures of technological dependence.

Cybersecurity and Preparedness

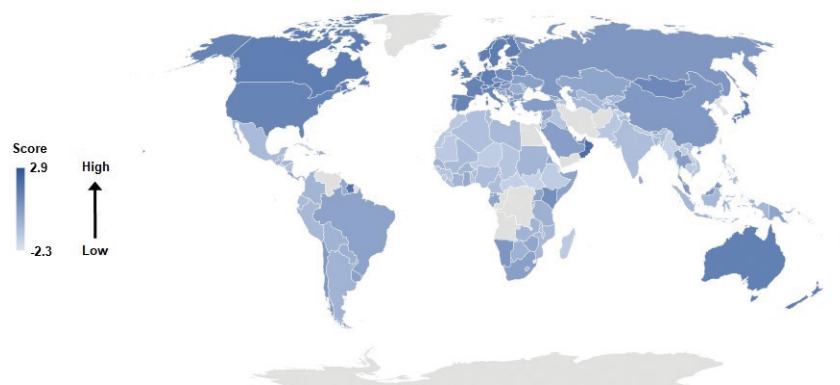
Good cybersecurity practices can reduce national systemic cyber risk exposure. The majority of the financial system is privately owned, and securing the individual institutions is primarily their own responsibility. However, national governmental institutions play a critical role in preventing

TABLE 2

Cyber Threat Assessment Criteria

	Nation States	Proxies	Cybercriminals	Hacktivists
High	<ul style="list-style-type: none"> - Had critical infrastructure destroyed by sophisticated cyber means, likely only available to a nation-state - Financial sector was specifically affected by disruptive or destructive cyberattacks assessed to be from a nation state - Financial institution lost significant amounts of funds as the result of a nation-state’s cyber enabled fraudulent activities 	<ul style="list-style-type: none"> - A frequent proxy target from multiple campaigns or groups. Likely under “constant assault” - A proxy campaign is believed to have targeted critical infrastructure in this country - Numerous campaigns or groups believed to target the financial sector in this country - Proxies have demonstrated ability to destroy data or systems in this country 	<ul style="list-style-type: none"> - Cybercriminals have repeatedly and specifically targeted this country - Criminals have stolen large sums of money from institutions in this country - Cybercriminals repeatedly target financial institutions in this country - High level of malware infections in the country - Cybercriminals attacking this country believe they are beyond the reach of this country’s law enforcement 	<ul style="list-style-type: none"> - A frequent hacktivist target from multiple campaigns or groups. Likely under “constant assault” - Numerous campaigns or groups believed to target the financial sector in this country - Hacktivists have demonstrated ability to destroy data or systems in this country - Hacktivists have caused disruption to financial institutions operations through their attacks
Medium	<ul style="list-style-type: none"> - Targeting of critical infrastructure by cyber means that was of minimal impact - Financial sector was specifically targeted by a nation-state though minimally affected - Financial institution’s losses from nation-state attacks are moderate to minimal 	<ul style="list-style-type: none"> - An occasional proxy target, probably not under “constant assault” - Proxy campaigns are not believed to have originated in this country - Financial sector in country is occasionally targeted by proxies 	<ul style="list-style-type: none"> - Cybercriminals occasionally target this country - Moderate level of malware infections in the country - Cybercriminals regularly target the financial sector - Cybercriminals believe this country’s law enforcement could affect them, though persist regardless 	<ul style="list-style-type: none"> - Hacktivism exists but its targets are primarily opportunistic - Financial sector is A sporadic target of hacktivist attacks
Low	<ul style="list-style-type: none"> - No known targeting of critical infrastructure by another nation-state - No known targeting of the financial sector by a nation-state - No known losses from nation-state cyberattacks 	<ul style="list-style-type: none"> - No evidence of the country being a target of attacks by proxies - Financial sector not targeted by proxies 	<ul style="list-style-type: none"> - No notable examples of cybercrime specifically targeting this country - Cybercrime affecting the country is generally unsophisticated, relying on confidence scams or commodity malware - Cybercriminals believe this country’s law enforcement could affect them and therefore generally don’t specifically target this country 	<ul style="list-style-type: none"> - Minimal to no successful hacktivist attacks against financial sector institutions in country - Minimal to no hacktivist activity within the country

FIGURE 6
Technology Dependence



SOURCES: World Bank Global FINDEX data base (retrieved 2019); and authors' research.

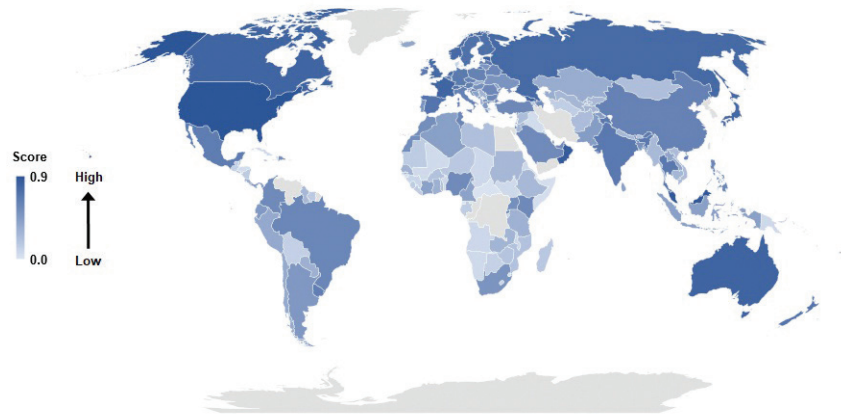
crises through sound laws and regulations and by helping quickly address a large cyber event before it becomes a crisis. Through effective incident-response actions by a national computer emergency response team (CERT), governments can help reduce the risk that a cyber incident in one or a few victim firms could spread widely. Governments can use their unique position to help improve the cybersecurity workforce through training programs, and they can improve companies' resiliency by facilitating public-private sharing of cybersecurity information. Governments that take these steps reduce their country's risk of systemic cyber events occurring.

Measuring cybersecurity. The measure used here for illustration is the Global Cybersecurity Index (GCI)³⁶—a survey performed by the International Telecommunication Union (ITU), the United Nations agency for information and communication technologies. The index, which measures the commitment of countries to strengthen cybersecurity, is quantified as a mix of quantitative and qualitative data. It comprises five pillars (legal, technical, organizational, capacity building, and cooperation) and computes index values for each.³⁷ ITU conducted a survey in 2017 to assess nations' commitment to cybersecurity, assessing each participating nation against the five pillars (see Figure 7). We apply this index as a proxy for the nation's level of cybersecurity.

Shock Resilience

The ability of a country's financial sector to absorb and reduce shocks is a critical component of its ability to handle cyber shocks specifically. In the case of a systemic cyber event, financial firms would incur losses (see previous sections), and their ability to absorb shocks depends on the

FIGURE 7
ITU Global Cybersecurity Index



SOURCE: ITU, “Global Cybersecurity Index (GCI),” 2017.

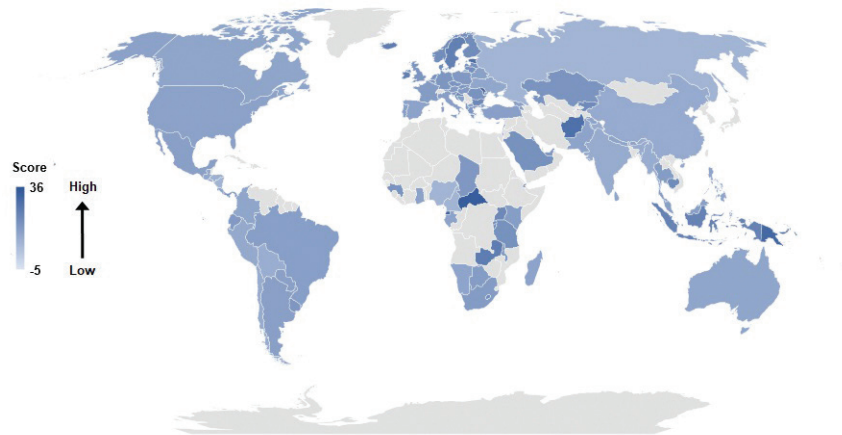
size and quality of their buffers. For illustration purposes, we assess in Figure 8 the banking system’s regulatory capital buffers in several countries, expressed as percent of Risk-Weighted Assets.

Systemic Cyber Risk Index

In a last step, we combine into an aggregate indicator of systemic cyber risk the three subindices presented in this section.³⁸ Using the illustrative data, we found that high levels of cyber threat and low levels of financial shock resilience characterize the countries most susceptible to systemic cyber risk. Conversely, countries with the lowest levels of systemic cyber risk have low levels of cyber threat and high levels of financial shock resilience. Their commitment to cybersecurity and their dependence on technology often oppose each other: one is positive while the other is negative. Trends have generally shown that societies’ dependence on technology is increasing rapidly—typically faster than the rate of increase in their commitment to cybersecurity.

Technology dependence plays an outsized role in the opportunity for a cyber event to become systemic. Governments, however, do not have much control over a country’s technology dependence other than using regulations to force organizations to have redundancies. Technology dependence is rising globally, albeit unevenly. With increasing dependence, cyber threat increases. It is likely that the increase in cyber risk exposure will be faster than the compensating cybersecurity improvements. This underscores the importance of shock resiliency mechanisms such as capital buffers in preventing systemic cyber risk from turning into a financial stability event.

FIGURE 8
Map of Financial Sector Shock Resilience (2017)

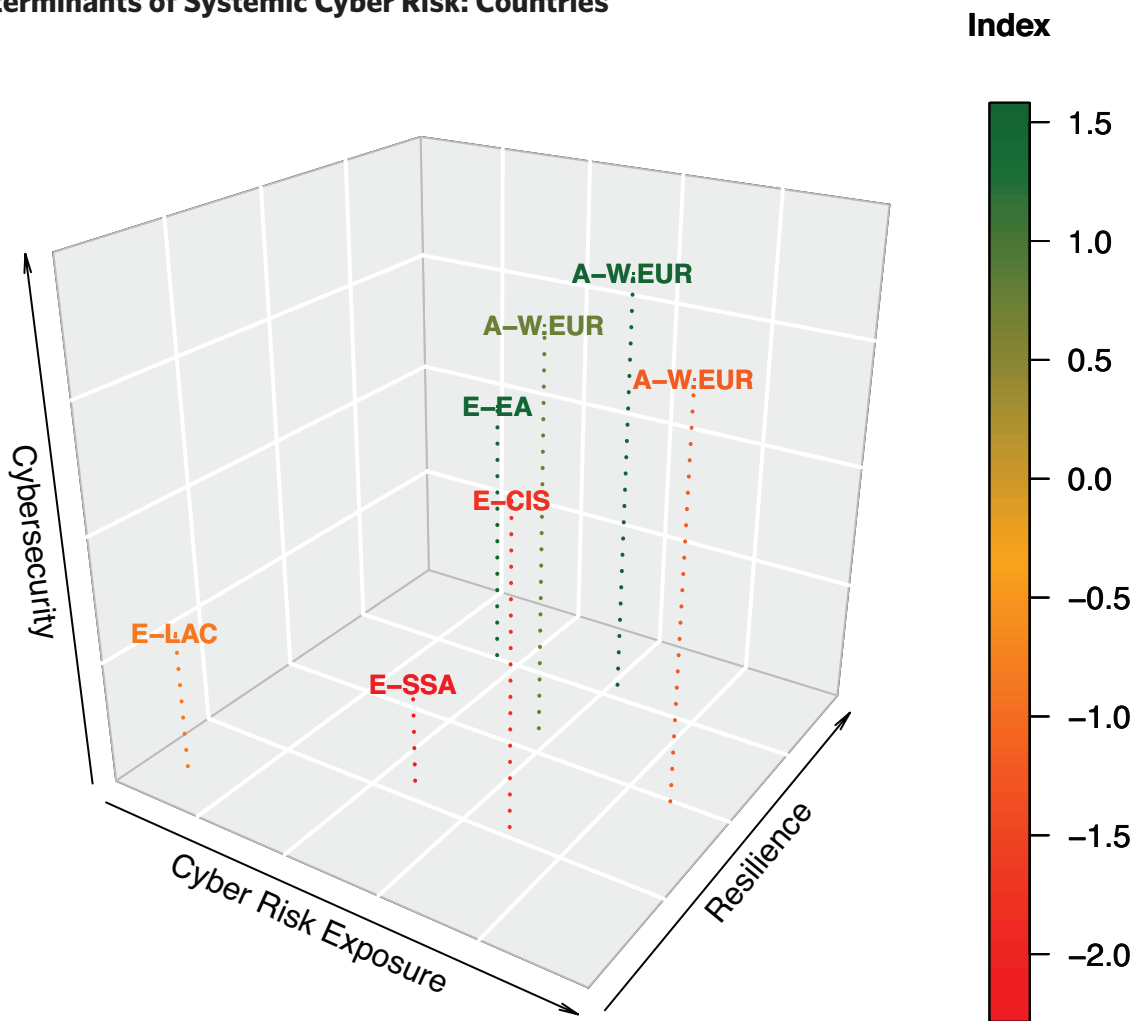


SOURCE: IMF Financial Soundness Indicators.

A case can be made for improving cybersecurity practices and beefing up buffers to absorb cyber shocks (Figure 9). Generally, advanced economies (A) are more exposed to systemic cyber risk as a result of high network connectivity. But such countries typically have better cybersecurity and higher (capital and liquidity) buffers in their financial systems. And this matters a lot. For instance, the emerging country (E) in sub-Saharan Africa (SSA), designated in the figure as E-SSA, basically has the same cyber risk exposure as two advanced economies in Western Europe, A-W.EUR. But in terms of systemic cyber risk, E-SSA scores poorly because of its weaknesses in cybersecurity practices and weak buffers in the financial system. The two other countries have a stronger commitment to increasing cybersecurity, and their financial institutions are better equipped to absorb shocks. Also, the level of development does not necessarily mean weaker cybersecurity or lower buffers, as can be seen in the case of a developing country in emerging Asia, E-EA. This country's exposure to cyber risk is similar to that of country E-SSA, yet its high financial-system resilience paired with its solid cybersecurity practices indicate that country E-EA has taken important steps to boost cybersecurity and that its financial system has excellent buffers. Countries that are heavily exposed to cyber risk, like the Group of 7 (G7) country A-W.EUR (depicted at the very right of the box), despite having very strong cybersecurity practices and decent buffers, still score poorly, suggesting that buffers in the financial system would need to increase if the country wanted to improve its systemic cyber risk score.

Another aspect of the illustration of systemic cyber risk index is proportionality. The emerging-market country in Latin America and the Caribbean, E-LAC (depicted in the very left of the box), has been less committed to improving cybersecurity and lacks substantial buffers in its financial system. Yet the country's systemic cyber risk score is about average. Put differently, compared to the

FIGURE 9
Determinants of Systemic Cyber Risk: Countries



SOURCE: Authors.

cyber risk the country is exposed to, cybersecurity levels appear reasonably high. But, clearly, higher buffers or better security would help boost the index score.

Ways to Mitigate Risk

Legal, technical, and organizational measures can be taken, aided by capacity building and international cooperation.³⁹ Having in place comprehensive legislation that covers both substantive

law and procedural law can go a long way. Legislation should also be formulated in a technology-neutral way⁴⁰ so that the rules are relatively immune to inevitable changes in technology (i.e., laws should not be designed in a way that they only apply to specific technologies). Furthermore, national legislation needs to be compatible and, to the extent possible, harmonized with international law to form the basis for cross-border cooperation. The Budapest Convention on Cybercrime has become the starting point for many countries' legal framework for cybersecurity.

Organizational and institutional setups can be strengthened. Today, most countries already have or are in the process of formulating a cybersecurity strategy. This often includes the national security dimension of cyber risk. The institutional approach has crystallized as an effective measure to coordinate and implement cybersecurity strategies.⁴¹ One or more dedicated agencies approve plans, programs, reports, procedures, principles, and standards. The agencies then ensure proper application and implementation while fostering coordination.

Strong institutions that quickly adapt to the changing landscape are important to successfully mitigate systemic events. Governments that invest in institutions and prioritize cybersecurity not only improve the resiliency of their government but also increase the likelihood they will be able to quickly react to an emerging cyber crisis before it causes a financial crisis. Similarly, strong governmental financial institutions undergird the country's financial stability and reduce the likelihood that a large cyber event would have the opportunity to threaten that stability.⁴²

At the national level, proactive measures that bring the public and private sectors together have proven helpful. One example is a national-level cyber exercise wherein a hypothetical systemic scenario is played out with both government agencies and representatives from the private sector. Exercises both help improve resilience to specific scenarios and improve the interaction and relationships needed to resolve those scenarios. Another example is establishing mechanisms for cyber threat information sharing between public- and private-sector organizations, which immediately improve firms' resilience, especially firms with fewer resources to provide for their own security.

Government financial institutions play critical roles in ensuring resilience to cyber-enabled shocks. Central banks and ministries of finance have many options to mitigate the impact of a shock. Central banks can inject money into an institution or market that had a victim organization lose significant liquidity due to large-scale malware-enabled fraud, or a situation of trapped liquidity due to a massive ransomware infection. Authorities can provide assurances to the public to calm fears and prevent panic. Government institutions can provide emergency means for clearing and settling or for providing grace periods if a victim firm were unable to do so because of a cyber attack. If the

strength of these institutions could be quantitatively assessed, it would be a beneficial addition to this framework.

Conclusion

Cyber risk—in particular its systemic nature—has been poorly understood and accounted for. An important component is understanding the country-level exposure to systemic cyber risk. To that end we have proposed a novel framework for evaluating a country's systemic cyber risk level and have provided an illustrative index to show what could be done if a more thorough evaluation were performed with more reliable data.

By working through this in-depth and deliberate systemic cyber risk assessment exercise, individual organizations would be better able to understand their risk exposure to systemic cyber risk and thus take actions to decrease the risk to acceptable levels. Additionally, governments could use this methodology (or a modified version of it) to improve laws and policies, strengthen institutions, and create, implement, and test plans that improve national-level resilience to systemic cyber risk.

BOX 2

International Norms and Agreements

Given the potentially disruptive impacts of direct targeting in the event of conflict, advocates call for protecting the global financial system from such targeting. In 2015, the United Nations General Assembly published a report that calls for norms in cyberspace and specifies certain standards regarding critical infrastructure:

“A State should not conduct or knowingly support ICT [information and communications technology] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.”⁴³

Also, the Carnegie Endowment for International Peace in their work focusing on the Group of 20 (G20) proposed specific language for an agreement specific to the financial system:

“A State must not conduct or knowingly support any malicious use of ICT that could undermine security and confidence and endanger financial stability, such as by manipulating the integrity of data and algorithms of financial institutions or undermining the availability of critical financial systems.”

“To the extent permitted by law, a State must respond promptly to appropriate requests by another State to mitigate such activities, such as undermining the availability of critical financial systems or manipulating the integrity of financial institutions’ data and algorithms, when such activities are passing through or emanating from its territory or perpetrated by its citizens.”⁴⁴

As the authors state in the paper, such an agreement would “make explicit what could be considered emerging state practice.”

Additionally, Microsoft, in “A Digital Geneva Convention to Protect Cyberspace,” proposes as the second point that nations should in peacetime:

“refrain from attacking systems whose destruction could damage the global economy (e.g., integrity of financial transactions), or otherwise cause major global disruption (e.g., cloud-based services).”⁴⁵

Notes

- ¹ International Telecommunication Union (ITU), “Global Cybersecurity Index (GCI) 2017,” 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
- ² Phil Warren, Kim Kaivanto, and Dan Prince, “Could a Cyber Attack Cause a Systemic Impact in the Financial Sector?,” Bank of England, Quarterly Bulletin, 2018, <https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2018/could%20a%20cyber%20attack%20cause%20a%20systemic%20impact%20final%20web>.
- ³ Tom Bergin, “SWIFT Says Bank Hacks Set to Increase,” Reuters, September 26, 2016, <http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11W1XY>.
- ⁴ Calsoft, “Internet of Things (IoT) 2018—Market Statistics, Use Cases and Trends,” 2018, <https://calsoftinc.com/resources/ebooks/internet-of-things-iot-2018-market-statistics-use-cases-and-trends/>.
- ⁵ IHS Markit, “IoT Trend Watch 2017,” 2017, <https://cdn.ihs.com/www/pdf/IoT-trend-watch-2017.pdf>; and IHS Markit, “IoT Trend Watch 2018,” 2018, <https://cdn.ihs.com/www/pdf/IoT-Trend-Watch-eBook.pdf>.
- ⁶ While ex-ante regulation can help introduce minimum standards, the verdict is still out regarding to what extent software developers should assume ex-post liability for damage caused by the flawed product.
- ⁷ R. Böhme, “Security Metrics and Security Investment Models,” in *Advances in Information and Computer Security*, eds. I. Echizen, N. Kunihiro, R. Sasaki, IWSEC 2010, Lecture Notes in Computer Science, Vol. 6434 (Berlin and Heidelberg: Springer, 2010).
- ⁸ Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, “Cyber Risk, Market Failures, and Financial Stability,” International Monetary Fund Working Paper WP/17/185, 2017, <https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104>.
- ⁹ Atlantic Council, “Beyond Data Breaches: Global Interconnections of Cyber Risk,” Zurich Insurance Group, Risk Nexus, April 2014; World Economic Forum (WEF), “Understanding Systemic Cyber Risk,” Global Agenda Council on Risk & Resilience, White Paper, October 2016.
- ¹⁰ Daniel Coats, “Worldwide Threat Assessment of the U.S. Intelligence Community,” 2018, <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.
- ¹¹ Lyu Jinghua, “A Chinese Perspective on the Pentagon’s Cyber Strategy: From Active Cyber Defense to Defending Forward,” Lawfare, 2018, <https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward>.
- ¹² Damian Van Puyvelde, “Hybrid War: Does It Even Exist?” NATO Review Magazine, 2015, <https://www.nato.int/DOCU/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm>.
- ¹³ David Barno and Nora Bensaehl, “A New Generation of Unrestricted Warfare,” *War on the Rocks*, 2016, <https://warontherocks.com/2016/04/a-new-generation-of-unrestricted-warfare/>.
- ¹⁴ See TASS, “General Staff: A Feature of Future Conflicts Will Be the Use of Robots and Space Tools,” <https://tass.ru/armiya-i-opk/5062463>.
- ¹⁵ Atlantic Council, “Beyond Data Breaches: Global Interconnections of Cyber Risk,” Zurich Insurance Group, Risk Nexus, April 2014; Atlantic Council, “Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures,” Zurich Insurance Group, Risk Nexus, 2015.

- ¹⁶ Antoine Bouveret, “Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment,” International Monetary Fund Working Paper WP/18/143, 2018; McAfee, “Net Losses: Estimating the Global Cost of Cybercrime,” 2014; OECD, “Cybersecurity Policy Making at a Turing Point,” 2012. See also Atlantic Council, “Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures,” Zurich Insurance Group, Risk Nexus, 2015.
- ¹⁷ World Economic Forum (WEF), “Understanding Systemic Cyber Risk,” Global Agenda Council on Risk & Resilience, White Paper, October 2016.
- ¹⁸ Atlantic Council, “Beyond Data Breaches: Global Interconnections of Cyber Risk,” Zurich Insurance Group, Risk Nexus, April 2014.
- ¹⁹ Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, “Cyber Risk, Market Failures, and Financial Stability,” International Monetary Fund Working Paper WP/17/185, 2017, <https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104>.
- ²⁰ Office of Financial Research (OFR), “Cybersecurity and Financial Stability: Risks and Resilience,” OFR Viewpoint 17-01, 2017.
- ²¹ Columbia SIPA School of International and Public Affairs, “The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability,” December 2018.
- ²² For a discussion of CCPs, see F. Wendt, “Central Counterparties: Addressing Their Too Important to Fail Nature,” IMF Working Paper WP/15/21, 2015.
- ²³ European and U.S. regulators in 2016 achieved an agreement that links the CCPs across the Atlantic, thereby increasing redundancies and lowering systemic risk, aided by product standardization.
- ²⁴ Jack Stubbs, Pavel Polityuk, and Dustin Volz, “Cyber Attack Sweeps Globe, Researchers see ‘WannaCry’ Link,” Reuters World News, June 27, 2017, <https://www.reuters.com/article/uk-cyber-attack/cyber-attack-sweeps-globe-researchers-see-wannacry-link-idUKKBN1911TF>.
- ²⁵ Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” Wired—Security, August 22, 2018, <https://www.wired.com/story/notpetya-cyber-attack-ukraine-russia-code-crashed-the-world/>.
- ²⁶ Wavestone, “Cyber-Resilience,” Risk Insight, 2019, <https://www.wavestone.com/app/uploads/2018/01/2019-RiskInsight-VE.pdf>.
- ²⁷ Marsh, “NotPetya Was Not Cyber War,” Marsh and McLennan Companies, August 2018, <http://www.mmc.com/content/dam/marsh/Documents/PDF/pl/NotPetya-Was-Not-Cyber-War-08-2018.pdf>.
- ²⁸ Jason Healey, Patricia Mosser, Katheryn Rosen and Adriana Tache, “The Future of Financial Stability and Cyber Risk,” Brookings Cybersecurity Project, The Brookings Institution, October 2018.
- ²⁹ Bank for International Settlements (BIS), “Central Clearing: Trends and Current Issues,” BIS Quarterly Review, December 2015, https://www.bis.org/publ/qtrpdf/r_qt1512g.htm, highlights that interactions between CCPs and the rest of the financial system are less than perfectly understood.
- ³⁰ Jose Pagliery, “The Inside Story of the Biggest Hack in History,” CNN Business News, August 5, 2015.
- ³¹ Zurich Insurance Group, “Cyber Risks Scenario for Business: Counting the Cost of Growing Societal Threats,” December 18, 2017, <https://www.zurich.com/en/knowledge/articles/2017/12/global-risks-2017-cyber-risks-business-scenario>.

- ³² World Economic Forum (WEF), “Understanding Systemic Cyber Risk,” Global Agenda Council on Risk & Resilience, White Paper, October 2016.
- ³³ This scenario was proposed in Atlantic Council, “Beyond Data Breaches: Global Interconnections of Cyber Risk,” Zurich Insurance Group, Risk Nexus, April 2014.
- ³⁴ Robert Knake, “A Cyberattack on the U.S. Power Grid: Contingency Planning Memorandum No. 31,” Council on Foreign Relations, 2017, <https://www.cfr.org/report/cyberattack-us-power-grid>.
- ³⁵ World Bank Global FINDEX data base (retrieved 2019).
- ³⁶ The GCI is published by the International Telecommunication Union (ITU), the United Nations’ agency for information and communication technologies. In the survey, 134 countries responded to the questionnaire. A group of experts then weighted the questions and constructed the index. Countries that did not respond to the survey were given the opportunity to validate the ITU’s own estimates of the countries’ commitment to increasing cybersecurity.
- ³⁷ International Telecommunication Union (ITU), “Global Cybersecurity Index (GCI) 2017,” 2017, p. 9-11, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
- ³⁸ The data within this illustrative index of indices resulted in 112 countries having data for all four areas. Those countries missing data in any of the four domains were excluded.
- ³⁹ International Telecommunication Union (ITU), “Global Cybersecurity Index (GCI) 2017,” 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
- ⁴⁰ International Telecommunication Union (ITU), “Understanding Cybercrime: Phenomena, Challenges, and Legal Response,” September 2012, <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CybcimeE.pdf>.
- ⁴¹ Group of Seven (G7), “Fundamental Elements of Cybersecurity for the Financial Sector,” 2016, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; and Emanuel Kopp, Lincoln Kaffenberger, and Christopher Wilson, “Cyber Risk, Market Failures, and Financial Stability,” International Monetary Fund Working Paper WP/17/185, 2017, <https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104>.
- ⁴² Such was the case in Chile when the second-largest bank experienced a large cyber attack in which threat actors stole U.S.\$10million and destroyed thousands of computers, disrupting bank operations for days. Although this event was significant, it did not cause a national panic, due in large part to the country’s strong institutions, which prevented the event from growing into a financial stability event.
- ⁴³ United Nations, “Developments in the Field of Information and Telecommunications in the Context of International Security,” United Nations General Assembly A/70/174, 2015.
- ⁴⁴ Carnegie Endowment for International Peace, “Cybersecurity and the Financial System,” 2019, <https://carnegieendowment.org/fincyber/>.
- ⁴⁵ Microsoft, “A Digital Geneva Convention to Protect Cyberspace,” 2017, <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace>.



1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

[CarnegieEndowment.org](https://www.CarnegieEndowment.org)