

The Ties That Bind: A Framework to Assess the Linkage Between Cyber Risks and Financial Stability

Jason Healey, Patricia Mosser, Katheryn Rosen, Alexander Wortman

December 2018

There is quite a bit of shared misery between practitioners protecting against another financial meltdown and those striving to keep their organizations safe from cyber attack and ensuring the Internet is resilient. Both the financial system and the interconnected networks of cyberspace are inherently complex, fragile, and at risk.

Now, these two systems—finance and the cyberspace—are not just interconnected but interdependent. The modern financial industry cannot work without a functioning Internet just as the organizations which keep the Internet secure need the finance sector to be strong. Fortunately, research on cyber risks to financial stability has grown significantly in recent years, as we summarize in a previous paper.¹

This working paper contributes to those efforts by presenting an analytical framework to assist those assessing how a particular cyber risk (such as a major distributed denial of service attack or DDoS) might initiate an episode of financial instability, or the reverse, how financial vulnerabilities in a particular part of the system (say the payments system) might be targeted by various kinds of cyber incidents. The analytical framework is high-level, intended to guide discussions on the linkages between the two sectors, particularly those which might cause contagion across the financial system. The paper begins with a short section on financial stability and how cyber risks differ to those normally faced by the sector. We then provide an overview of the general model through four main sections: cyber risks, financial

Project on Cyber Risk to Financial Stability (CRFS)

This working paper is the latest in a series of research by Columbia University's School of International and Public Affairs (SIPA). This has been a collaboration between SIPA's Initiative on Central Banking and Financial Policy and the Initiative on Cyber Risk.

Over the past two years, this project has hosted a series of engagements bringing together industry experts from financial institutions, regulators and other policymakers, and academics and practitioners with backgrounds in finance and cybersecurity. The authors wish to thank the participants in those workshops as well as those who have provided advice and background.

This paper builds on (and partially summarizes) an earlier SIPA-authored publication, "The Future of Financial Stability and Cyber Risk," published by the Brookings Institutions in October 2018.

stability, the "transmission channels" by which cyber risks can induce financial turmoil, and the amplifiers and dampeners which shift the balance of risks. The Appendix provides a set of questions that enables users to establish a baseline understanding of a particular market and to probe further each component of the framework as it relates to that market.

Understanding Finance and Cyber

The financial system performs various functions such as facilitating payment and settlement, allocating credit, transferring risk, and providing liquidity. Significant impairment of any of these core functions can cause financial instability. Therefore, financial stability authorities are concerned with how financial markets and institutions can propagate and amplify shocks, regardless of their source. Particularly, these authorities are focused on vulnerabilities which cause the system to be fragile and subject to periodic crises and runs. Since the timing and specific triggers of crises are hard to predict, experts in financial stability focus less on the shocks and triggers of crises, and more on vulnerabilities and propagation mechanisms that make the system unstable in the first place.

Although capable of causing widespread harm, traditional financial shocks tend to arise out of self-preservation or mistakes, rather than malice. A trader trying to corner the market is not seeking to destroy or disrupt the entire system. Likewise, policymakers can make mistakes or misjudge the impact of their policies, but do not act with the purpose of creating financial turmoil. Cyber shocks, in contrast, could be intentional

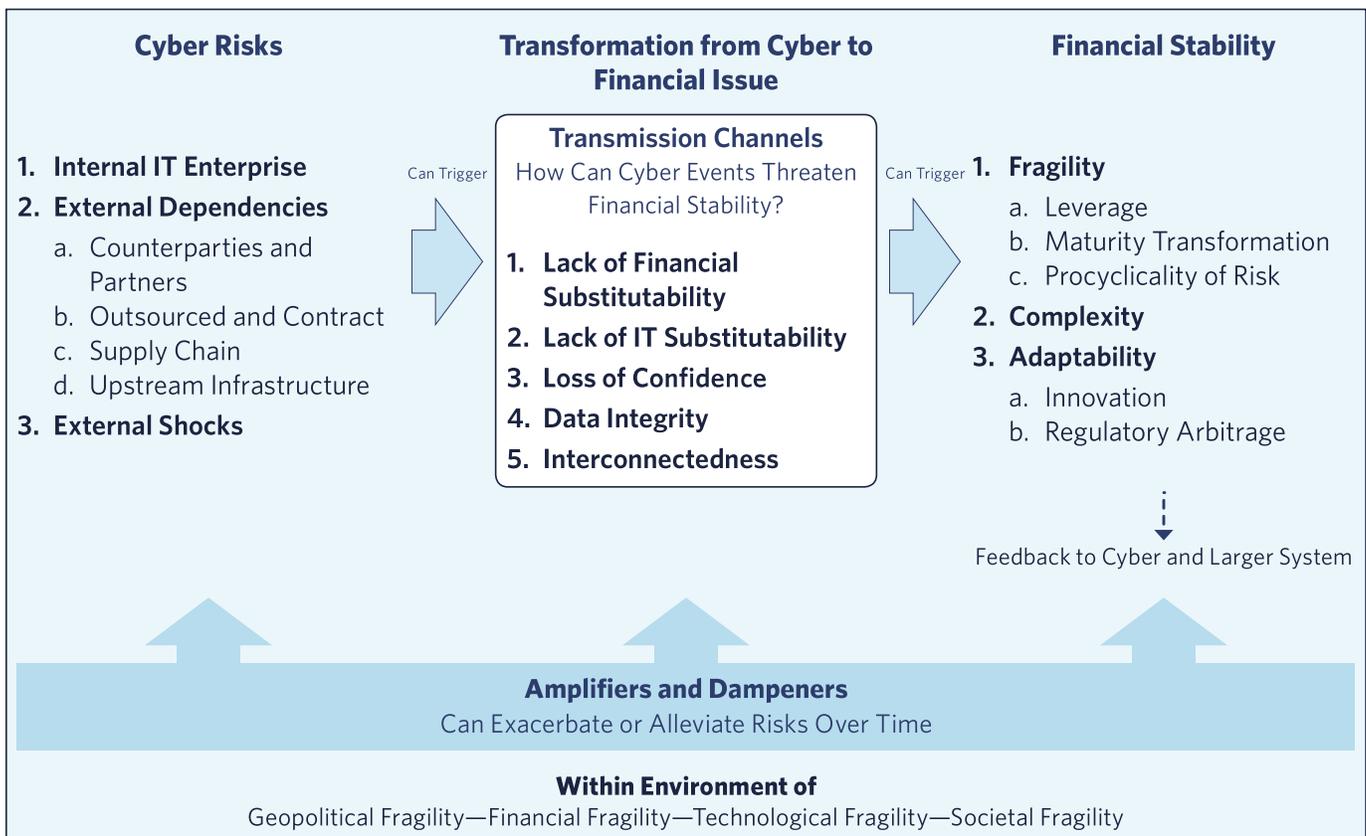
acts by an adversary to target vulnerable areas of the financial system and deliberately initiate financial instability or to give a push to an economy teetering on the edge of collapse, to initiate or extend a crisis.

Framework on Cyber Risks to Financial Stability

The remainder of this working paper outlines an analytical framework to facilitate structured analysis of how cyber risks might induce systemic financial instability. It is a model for systemic risk rather than just for single enterprises, designed to be repeatable and adaptive, as well as market and technology agnostic.

The graphic below illustrates the basic framework, with risks flowing from left to right. Cyber risks can stem from one of several “aggregations” (on the left) which can then trigger a financial stability incident (right) through the transmission channels (center). Each category is affected by amplifiers and dampeners which can exacerbate or alleviate them, all within an environment of inherent fragilities (bottom).

The risks flow from left to right: the cyber risks from the left side can, through the transmission channels,



become systemic financial risks. However, the framework can be used in several ways depending on the specific analytical need.

To assess the financial risk from a particular kind of cyber incident, analysis should proceed *left to right*. For example, an outage at a major cloud service provider would be a vendor-availability issue which may affect financial stability primarily through lack of IT substitutability (but perhaps also confidence and interconnectedness). The financial stability impact will depend on business and technology decisions taken in response to the attack as well as the spillover effects those decisions have on other markets and firms. Under normal market conditions, even a significant disruption may not cause financial instability. But would the outage cause different responses or different spillovers to the rest of the financial system if markets or the economy are particularly fragile, for example if leverage is high and asset prices are falling?

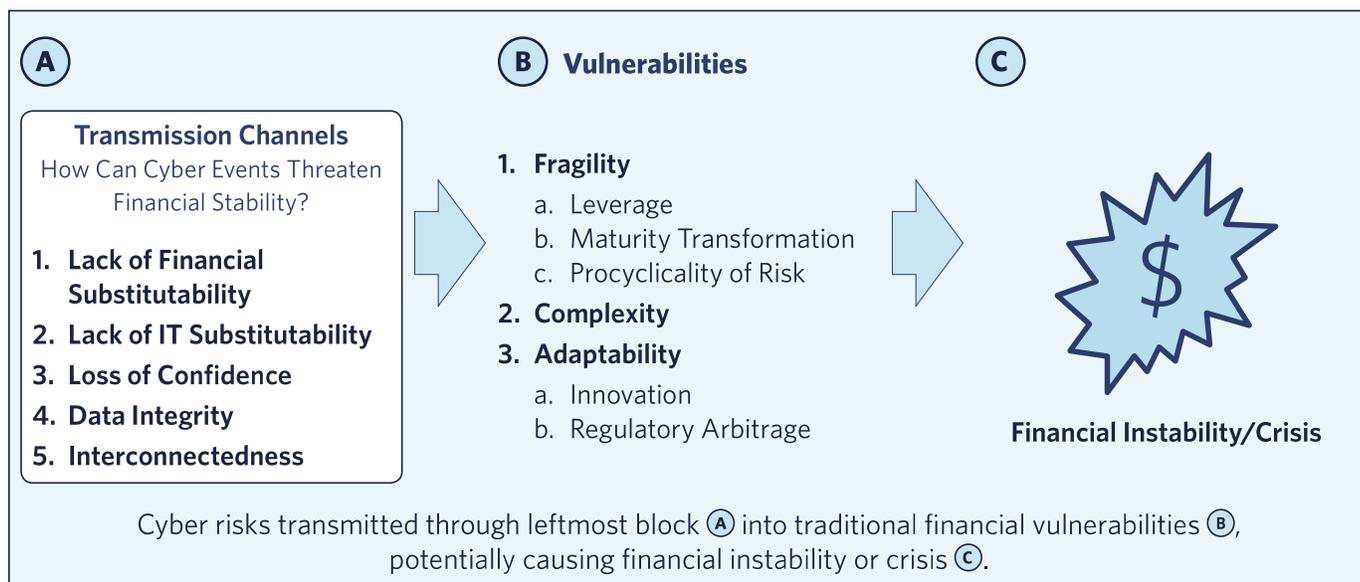
To assess how a particular aspect of the financial system might be affected by a wide range of cyber incidents, analysis should proceed from *right to left*. As one example, the triparty repo market is a key financial funding market providing leveraged maturity transformation to many financial firms using a very small number of critical market infrastructures (lack of financial and IT substitutability). What cyber risks might have a large direct impact on this market, and which types of cyber attacks are more likely to cause contagion and a destabilizing pullback in funding? How could a hostile adversary time a cyber incident to trigger or exacerbate financial vulnerabilities in this market?

To assess the impact of amplifiers and dampeners to the system, analysis should proceed from the *bottom up*. This leads to important questions, such as how will new technologies like blockchain exacerbate or alleviate risks to particular financial markets or institutions? How will breakdowns (or, less likely, improvements) to international regulation and governance of financial and cyber risks affect the overall stability of the system?

Financial Stability Risks and Vulnerabilities²

The framework includes an assessment of vulnerabilities, key characteristics of the financial system which can propagate and amplify shocks and thus can lead to instability or in the extreme a crisis. The model emphasizes three sources of this contagion: fragility, complexity, and adaptability.

Fragility is one of the most important concepts in financial stability and includes three core characteristics of financial systems that contribute to systemic vulnerability: leverage, maturity transformation, and the procyclicality of risk. Leverage refers to being highly indebted at the level of the institution, market participant, or position. More levered investors or institutions have larger losses (gains) for any fall (rise) in the value of their assets. Maturity transformation is the process of financing illiquid, longer-term assets with short-term, money-like liabilities (e.g. buying long-dated mortgages with deposits or short-term borrowing).



Greater maturity transformation makes an institution or investor more vulnerable to a pullback in short-term borrowing. Procyclicality of risk results from the actions market participants take in self-preservation of positions. For example as asset prices fall, the cost of funding (borrowing) rises as the value of the collateral of the borrower is falling. Associated losses can cause some investors and institutions to sell assets, putting further downward pressure on asset prices. Declining asset prices and losses also increase the risk to short-term lenders who reduce the amount of funding they provide, causing the value of risky assets to fall even further. In the extreme, the interaction of these three characteristics can result in a feedback loop of large asset price declines, growing losses, and accelerated loss of short-term funding, in essence, a run.

Complexity refers to the inherent interconnectedness of the web of markets, contracts, and institutions that are difficult to understand and model, and which allow shocks to propagate through the financial system, impacting sectors and activities that are not directly tied to the original shock. Obviously, the inherent (and growing) complexity of the financial systems means that, as in 2008, risks can cascade in unpredictable ways.

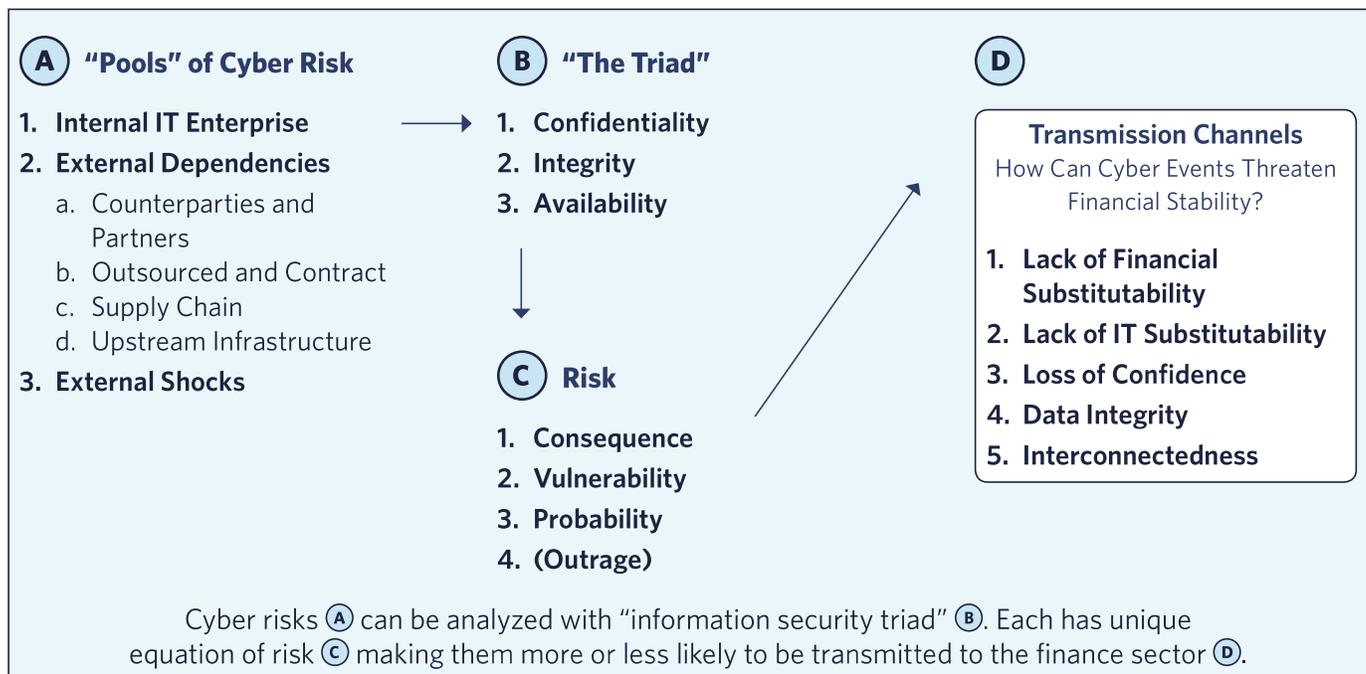
Adaptability includes mechanisms and innovations that foster a dynamic and evolving financial system but can become vulnerabilities, including regulatory

arbitrage. Innovation is the ability for market participants to push the envelope with new products, markets, and institutions which can be beneficial but can also increase the chances of crises. Innovations in some mortgage securitizations and related derivatives in the 2000s are notorious examples. Often innovation deliberately finds gaps in regulation. This is regulatory arbitrage, the incentive to shift financial products and services to firms outside traditional regulatory constraints, as is now happening with some fintech.

Cyber Risks

There are many ways to analyze cyber risks but most tend to focus on risks inside a single enterprise, rather than across a system. This paper borrows an approach from an Atlantic Council paper which slices the risks by “aggregations,” where the risks may pool far outside the enterprise.³ These aggregations can broaden traditional thinking about risks. Each threatens confidentiality, integrity, and availability in specific ways with a unique set of consequence, vulnerability, probability, and outrage.⁴ This last factor, outrage, is not often included as a cyber risk, but included here to directly tie to the potential loss of public confidence.⁵

Different organizations may have their own factors to understand and measure cyber risks. Those factors can



be substituted for the factors outlined in this framework so long as the substitution leads to clarity in the effect on the transmission channels.

Aggregations or “Pools” of Cyber Risks—Cyber risk can pool in three distinct ways. Many but not all cyber risks are in an organization’s own IT systems. This is reminiscent of financial risk, where a failure can cascade even to organizations which themselves might have made responsible risk decisions. As organizations are more interconnected and have more external dependencies, the importance of these external sources of risk increases. The main pools can be generalized to those internal to the organization’s own IT enterprise, those on which they depend, and external shocks.

Internal IT Enterprise is the cumulative set of an organization’s (mostly internal) IT infrastructure to include hardware, software, servers, and devices as well as related staff and processes. This is by far the most well understood pool of risk. It is well measured, is the daily experience of most cybersecurity practitioners, and is the main area of innovation and new cybersecurity products.

External Dependencies are just as important, however much they are overlooked by many enterprises. They include a growing array of third-parties, utilities, and infrastructures an organization relies upon to conduct its functions. Organizations tend to have far less visibility of and ability to manage these risks.

Counterparties and partners include dependence on, or direct interconnection with an outside organization such as trading counterparties and joint ventures. Outsourced and contract is risk from contractual relations with external suppliers such as human resources, legal, data, or IT. Supply chain includes both risks to supply chains for the IT sector and cyber risks to traditional supply chains and logistics. This can stem from tampered products or disrupted distribution networks. Upstream infrastructure is the risk from disruptions to infrastructure relied on by economies and societies, especially electricity, finance, and telecoms.

External Shocks, the third category of risks included in this model, are those from incidents outside the system, outside of the control of most organizations and which are especially likely to cascade. Major international conflicts or malware pandemics can cause or aggravate existing risks.

Information security risks in these pools can be analyzed using the traditional “information security triad” of confidentiality, integrity, and availability. **Confidentiality** is guaranteeing restrictions on information access, including methods to secure privacy and proprietary information. This is threatened by data breaches or other unauthorized access. **Integrity** is guarding against illicit alterations or destruction of information and assuring non-repudiation and authenticity. **Availability** is preserving timely and dependable access and use of information against Internet Service Provider outages or DDoS attacks.

The model gauges the severity of the risk factors due to potential consequence, vulnerability, probability, and outrage associated with any given cyber event. **Vulnerability** is a weakness in a system, operational procedure, or implementation that might result in an event. **Probability** is the likelihood of the occurrence of that event. **Consequence** refers to the degree of adverse impact from an event. **Outrage** is generally “how upset it’s likely to make people” which can overlap with consequence but ties to risk communication and loss of confidence.⁶

Transmission Channels: Linking Cyber Risks and Financial System Vulnerabilities

The presence of an aggregation of cyber risks and an inherently fragile financial system in and of themselves will not lead to an event of financial instability. The framework relies on transmission channels to serve as the link between the aggregation or cyber risk and financial vulnerabilities. These channels can cause feedback loops to accelerate or dampen instability. To varying degrees, the severity of these channels depends on the risk management and business decisions made in both finance and IT, for example, the preparedness and response to a cloud outage or trading posture in an environment of corrupted or compromised data.

In 2017, the US Department of the Treasury’s Office of Financial Research highlighted several “channels” through which cyber risks could be transmitted to the system, potentially leading to systemic crises.⁷ SIPA’s CRFS Project unveiled additional channels that are included as part of our analytical framework.

1. **Lack of Financial Substitutability**—Markets often run through a small number of service providers or have a select few institutions performing certain critical functions which can't be easily replaced. These are single points of failure for markets as they provide irreplaceable functions such as central counterparties, custodial and clearing bank services, exchanges and triparty repo, etc.
2. **Lack of IT Substitutability**—The financial system relies on technology and telecommunication, but this infrastructure has numerous single points of failure. This includes specific companies that provide critical services (such as cloud computing), key functions (such as internet exchange points and submarine cables) and even key communications protocols (like BGP).

Other Papers on Cyber Risk to Financial Stability

The **Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO)**, the global regulatory body for payments and securities regulators, released “Guidance on Cyber Resilience for Financial Market Infrastructures (FMI)” in 2016, highlighting the unique characteristics and threats of cyber risk to FMIs.

The **Bank for International Settlements (BIS)**, the “central bank for central banks” issued “Regulatory Approaches to Enhance Banks’ Cyber-Security Frameworks” in 2017, detailing specific regulatory and supervisory initiatives on cyber risk in four jurisdictions: Hong Kong, Singapore, the United Kingdom, and the United States. The BIS oversees the Basel Accords on global financial risk.

The **Institute of International Finance (IIF)**, a global financial services trade association, issued “Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System” in 2017, underscoring that cyber-attacks do not stop at borders and international efforts are needed to respond to them.

The **International Monetary Fund (IMF)** published a working paper “Cyber Risk, Market Failures, and Financial Stability” in 2017, emphasizing how cyber risks are unique and providing specific recommendations for effective regulatory policy.

The **Financial Stability Board (FSB)**, an international body that monitors the global financial system, created a “Cyber Lexicon Consultative Document” in 2018 for a common lexicon to foster better understanding of relevant cyber terminology and facilitate financial stability risk management practices. The FSB was created by the G-20 leaders after the financial crisis to promote financial stability.

The **Financial Stability Oversight Council (FSOC)**, a US federal government organization created in 2010 to monitor excessive risk to the US financial system, has been analyzing cyber security as a primary risk to financial stability since 2012. In its “Annual Report 2017,” the FSOC stressed several practical solutions, including automated sharing of cyber-security information; regulatory harmonization of a risk-based approach; additional regulation of third-party service providers; and continued exercises and work on sector-wide plans for recovery and response.

The **Carnegie Endowment for International Peace**, the think tank in Washington D.C., has a paper series on “Cyber-security and the Financial System,” including a proposal to the G-20 advancing a “Global Norm Against Manipulating the Integrity of Financial Data.”

The **Office of Financial Research**, a bureau within the US Treasury Department tasked with providing administrative, technical, and budgetary analysis, authored “Cybersecurity and Financial Stability: Risks and Resilience,” in 2017 that identified three ways cybersecurity incidents could threaten financial stability.

Columbia University’s School of Public and International Affairs (SIPA) published an earlier work summarizing much of the existing research and projects, summarizing both cyber risks and financial stability, and provided recommendations. This paper was published by Brookings as “The future of financial stability and cyber risk” in 2018.

3. **Loss of Confidence**—It is difficult to predict the point where market participants lose confidence in the market and the safety of their investments. The key question becomes at what point do investors or lenders no longer trust that they understand the risks in the system or have faith in institutions and decide to pull their funds, causing a traditional “bank run.”
4. **Data Integrity**—The trustworthiness of transaction and personal data is foundational for the financial system to function. A breach, corruption, or destruction of data can cause distrust in the integrity of the data thus, slowing or even halting financial transactions and flow of funds.
5. **Interconnectedness**—There are deep interconnections within both the financial system and IT infrastructure, which both rely on a complex, global web of infrastructures and partnerships to operate. The growth of electronic algorithmic trading is an example of these two systems becoming further intertwined.

Amplifiers and Dampeners of Transmission

The framework emphasizes amplifiers and dampeners as a key consideration to any analysis of risks and contagion. Over time, different factors will amplify or dampen the cyber and financial risks and vulnerabilities impacting the likelihood and severity of transmission. The amplifiers tend to make the system more fragile by speeding up transmission compared to the earlier state, the dampeners less so by slowing or even preventing such transmission. The worst case is when the amplifiers have a positive feedback mechanism, or behave procyclically, to magnify their impact which can cause systemic instability quite quickly.

Some of the amplifiers and dampeners will be particular to individual technologies, firms, markets, and businesses. Others are likely to have a more global impact and should be considered in any analysis of cyber risk to financial stability. Due to this difference in scale and impact, the framework identifies a series of high-level trends and controls of operational, technological, structural, behavioral, and policy-driven amplifiers and dampeners. Table 1 provides a few examples of such amplifiers and dampeners.

TABLE 1: EXAMPLES OF AMPLIFIERS AND DAMPENERS

TABLE 1: EXAMPLES OF AMPLIFIERS AND DAMPENERS						
CYBER			FINANCIAL			
	Technology	Operational	Policy	Structural	Behavioral	Policy
AMPLIFIERS	<ul style="list-style-type: none"> ▪ Increased IT complexity and dependence ▪ Single points of IT failure ▪ Cloud computing (increases concentration and vendor risks) 	<ul style="list-style-type: none"> ▪ Data localization requirements ▪ Diversified cyber crime markets 	<ul style="list-style-type: none"> ▪ Decreased international cooperation and governance ▪ Increase in nation-state attacks 	<ul style="list-style-type: none"> ▪ Leverage ▪ Maturity transformation ▪ Single points of failure (market infrastructure) 	<ul style="list-style-type: none"> ▪ Procyclicality of risk (herd mentality) ▪ Statistical risk (measurement and modeling) 	<ul style="list-style-type: none"> ▪ Regulatory arbitrage ▪ Statistical risk-based capital standards ▪ Fair value accounting
DAMPENERS	<ul style="list-style-type: none"> ▪ End-to-end encryption ▪ DDoS mitigation ▪ Cloud computing (decreases most other cyber risks) 	<ul style="list-style-type: none"> ▪ Finance sector cybersecurity collaboration ▪ Cyber risk ratings and insurance ▪ NIST Cyber Risk Framework 	<ul style="list-style-type: none"> ▪ International treaties (Budapest Convention) ▪ International norms 	<ul style="list-style-type: none"> ▪ Risk Limits ▪ Circuit breakers ▪ Initial margin 	<ul style="list-style-type: none"> ▪ Arbitrage (“Buy Low, Sell High”) incentives which balance crashes and booms 	<ul style="list-style-type: none"> ▪ Countercyclical capital regulation ▪ Liquidity regulation ▪ Activity restrictions ▪ 3rd party vendor regulatory compliance

SIPA's CRFS Framework provides a set of questions that enables users to establish a baseline understanding of the particular market being analyzed and to probe further each component of the framework as it relates to the market. As the framework is meant to be market and technologically agnostic, these questions allow users to account for specific vulnerabilities and features that are particularly influential in the market, for example infrastructure, key participants, fund flows, and IT dependence. This analysis will inevitably affect decision making processes at the business level and in securing IT.

Background Market Structure

These questions are useful for understanding the general components of the market to be analyzed and can drive further questions of both the financial and cyber risks.

1. Who are the key market participants and why and for what purpose do they use the market (e.g., hedging, long-term investment, speculation, financing, etc.)?
2. What is the degree of digitization of the market?
3. What are the key financial market and technology infrastructures, by importance, organization, and structure?
4. What are the key market characteristics, particularly with respect to risk taking and risk management?
 - a.) What is the market size and breadth of market activity including, participants?
 - b.) How is the structure and risk of financial instruments characterized: highly standardized, highly customized, what degree of complexity, what is the risk profile?
 - c.) What is the structure of transactions: over-the-counter, exchange traded, private (lending transaction), bilateral contracts, centrally cleared?
 - d.) How available and transparent are prices?
5. Which markets (or firms) are particularly closely interconnected?
 - a.) Which firms are particularly interconnected within the market?
 - b.) Which infrastructures are relied upon for market functioning?
 - c.) Which adjacent or related markets are particularly impacted?

Financial Stability Risks and Vulnerabilities

Financial stability analysis typically focuses on key characteristics which make financial systems fragile and subject to periodic crises: Financial Fragilities, Complexity, and Adaptability.

1. **Financial Fragilities:** Leverage, maturity transformation, and procyclical risk-taking:
 - a.) What is the typical balance sheet leverage for key participants: does it vary over time (or within the day)? What other types of leverage are used?
 - b.) What is the relative duration of assets versus liabilities for key participants?
 - c.) What are the risk and liquidity profiles of their assets, e.g. securities vs. loans?
 - d.) What is the liquidity profile of derivatives and borrowing activity, e.g. sensitivity to margin calls?
 - e.) What is the risk appetite of key participants?
 - f.) What are the business decisions when risk limits are breached and who makes those decisions?
 - g.) To what degree is herd mentality represented in the market?
2. **Complexity**
 - a.) How many steps are required for a typical trade—from execution to settlement?

- b.) Which steps are particularly complicated in terms of number of decision makers, number of firms or vendors, or dependencies on many infrastructures or technologies?
- c.) What are the funding needs and the drivers of risk management/business decisions at critical steps?

3. Adaptability

- a.) Are there segments of the market (or participants) with (rapidly) increasing activity, or with decreasing activity? What are the key drivers of these changes?
- b.) Describe regulatory requirements and significant differentials across key participants. Are regulatory requirements driving activity in certain products, with certain firms, or for certain customers?
- c.) Are the Financial Fragilities (defined above) shifting to other parts of the financial system in response to regulation?
- d.) What are the key technological advantages and financial innovations (if any) realigning activity in this market?

Pools of Cyber Risk

There are many ways to analyze cyber risks. Because many focus on risks inside a single enterprise, rather than across a system, this discussion borrows from an Atlantic Council paper which slices the risks by risk aggregations, which may pool far outside the enterprise.⁸ Each has example questions drawn, where applicable, from the NIST Cybersecurity Framework.⁹

1. Internal IT Enterprise

- i. To what degree are systems dependent on a few key services or technologies, such as on employees' desktops or servers in data centers?
- ii. To what extent is access to assets limited to the appropriate users and properly administrated and monitored?
- iii. What are the processes in place to manage timely software patches and updates?
- iv. How effectively can the firm respond to incidents and learn from the process?

2. External Dependencies

a.) Counterparties and Partners

- i. Do a significant number of partners share privileged access to any internal networks?
- ii. What vulnerabilities exist that could allow malware spread directly between any interconnected networks with external partners?

b.) Outsource and Vendors

- i. What is the scope of the risk horizon: are vendor bottlenecks identified, where a single provider services the majority of organizations in this space?
- ii. To what extent are business-critical functions outsourced to an IT or logistics provider?
- iii. What are the critical single points of failure and how can they be reduced?
- iv. To what degree are cybersecurity requirements enforced through contract or other formal agreement?

c.) Supply Chain

- i. How mature is the cyber supply chain risk assessment process in place? Is assessment of supply chain partners routine?
- ii. To what level are resilience requirements to support delivery of critical services established for all operating states (under duress, during recovery, and normal operations)?

d.) Upstream Infrastructure

- i. What is the probability and impact of outages to key infrastructure—such as the electrical grid, telecommunications network, or financial system? Are these incidents understood and scenarios rehearsed?

- 3. **External Shocks:** What are the risks outside the system, such as major international conflict or a global economic crisis?

The Triad

The principles of the “information security triad,” confidentiality, integrity, and availability, are central to most information security programs and assessments of risk. These can overlap with the elements in the risk equation (next section). For the given event or threat being analyzed:

1. **Confidentiality:** How do controls and protections ensure information is only accessed by those with the proper authority?
2. **Integrity:** How well does the system guard against modification or destruction of the system or information within it?
3. **Availability:** What controls does the system have for ensuring timely and reliable access to information?

Risk

Each kind of incident will have its own unique characteristics of risk, often expressed as an equation with the following elements:

1. **Vulnerability:** What are the weaknesses in the system that could fail or be exploited?
2. **Probability:** What is the likelihood of this vulnerability in fact failing or becoming exploited?
3. **Consequence:** What is the impact of such a failure or attack?
4. **Outrage:** How upset will important stakeholders (clients, employees, politicians) be from this failure or attack?

Transmission Channels— Cyber to Financial Stability

SIPA’s CRFS establishes five transmission channels that serve to link cyber risk and financial stability vulnerabilities. These mechanisms, in turn, can cause feedback loops to accelerate or dampen instability.

1. Lack of Financial Substitutability

- a.) What is the degree of market and infrastructure concentration? Are there single point or multiple points of failure?

- b.) What is the impact of rapid withdrawal by key participants?
- c.) What are the contingency plans for loss of key infrastructure?
- d.) Is there a presence of limits and/or backstops (e.g. financial, policy) at the firm-level or market-level?

2. Lack of IT Substitutability

- a.) What IT systems or software are business-critical to the market? If lost, what will be the impact on participation in this market? Will the firm’s decisions impact overall market functioning?
- b.) Are certain services concentrated in a single vendor, i.e., does a single cloud computing provider service a majority of the market?
- c.) Are there physical infrastructure systems (internet exchange points) or single companies or institutions for which failure would mean a critical vulnerability to financial markets?
- d.) Is their critical software used by participants (e.g. monoculture) across the market or sector?

3. Loss of confidence

- a.) Does the failure of a service or platform mean withdrawal of participation? Who is most likely to withdraw; which markets and firms are most impacted by a withdrawal?
- b.) Does a loss of confidence in institutions, trading, or communication platforms precipitate a halt in financial transactions and market flow? If so, which firms/market participants are most impacted? What is the impact on market pricing and particularly funding of key remaining participants?

4. Data Integrity

- a.) What are the critical data sources for the market to function?
- b.) What are the means of transmission of critical data?
- c.) For each critical data source, how would market functioning be impaired should that data be delayed, altered, corrupted, or destroyed?

- d.) For each critical data source, who relies on this information and how do they behave if the data were delayed, altered, corrupted, or destroyed?

5. Interconnectedness

- a.) What is the degree of overlap between key nodes of cyber risk and financial stability transmission? Where do the key nodes intersect?
- b.) What is the likelihood of common behavior (e.g. herd mentality, similarity of statistical risk measurement and modeling) across different types of participants, particularly in distress?
- c.) Is there a concentration of funding sources? How robust is funding?
- d.) Is there overlap of critical infrastructure in other markets?
- e.) What are the spillover effects?
- f.) What are the cross-border considerations?

- 6. What are the trade-offs in the sector from cloud adoption between increased cyber security but increased concentration and vendor risks?
- 7. What is the impact from the broad trend of decreasing international cooperation and governance?

Amplifiers and Dampeners

Over time, different factors will amplify or dampen the cyber and financial risks and vulnerabilities. The amplifiers tend to make the system more fragile compared to the earlier state, the dampeners less so.

Some of the amplifiers and dampeners will be particular to individual technologies, firms, markets, and businesses. Others are likely to have a more global impact and should be considered in any analysis of cyber risk to financial stability. A general list of this more global type would include those below.

1. Is there a trend towards increased concentration or fragmentation in the *technology*?
2. Is there a trend towards increased concentration or fragmentation in the *market* or *business*?
3. How is the financial system impacted by a general increase in national borders in cyberspace?
4. What is the impact from the general rise of fintech? Do these innovations add or remove fragility?
5. Do distributed ledgers add or remove fragility from the system?

About the Authors

Jason Healey is Senior Research Scholar at Columbia University's School of International and Public Affairs and Non-Resident Senior Fellow with the Cyber Statecraft Initiative of the Atlantic Council.

Patricia Mosser is Senior Research Scholar at Columbia University's School of International and Public Affairs and Director of the school's Initiative on Central Banking and Financial Policy.

Katheryn Rosen is Senior Research Scholar at Columbia University's School of International and Public Affairs and Non-Resident Senior Fellow with the Cyber Statecraft Initiative of the Atlantic Council.

Alexander Wortman received his Master of International Affairs at Columbia University's School of International & Public Affairs (SIPA), concentrating in International Finance & Economic Policy as well as Cybersecurity. He previously worked in journalism, covering US politics and defense issues for NHK (Japan Broadcasting Corporation) in Washington DC.

End Notes

1. Jason Healey, Patricia Mosser, Katheryn Rosen, and Adriana Tache, "The future of financial stability and cyber risk," Brookings, 10 October 2018, www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/. Also see the webcast of the launch event at the Atlantic Council, here: www.atlanticcouncil.org/events/webcasts/managing-cyber-risks-to-protect-financial-stability.
2. Common terms like risk and vulnerability are used in different ways by the financial and cyber communities. This paper uses terms like these somewhat interchangeably for better understanding between the two communities, even though it may be technically incorrect when used within a single community.
3. Jason Healey, "Beyond data breaches: global interconnections of cyber risk," Risk Nexus Report, Zurich Insurance Group and Atlantic Council, April 2014, www.zurich.com/_/media/dbe/corporate/docs/whitepapers/risk-nexus-beyond-data-breaches-global-interconnections-of-cyber-risk-2014.pdf
4. Definitions for confidentiality/integrity/availability and consequence/vulnerability/probability are derived from NIST: Michael Niels, Kelley Dempsey, Victoria Yan Pillitteri, "An Introduction to Information Security" NIST Special Publication 800-12: Revision 1, June 2017, <https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final>
5. Peter Sandman, "Introduction to Risk Communication and Orientation to this Website" 2014, www.psandman.com/index-intro.htm#overview. See Sandman's work for a full description of managing outrage as well as hazard.
6. Peter Sandman, "Introduction to Risk Communication and Orientation to this Website" 2014, www.psandman.com/index-intro.htm#overview. See Sandman's work for a full description of managing outrage as well as hazard.
7. Office of Financial Research, "Cybersecurity and Financial Stability: Risks and Resilience" Viewpoint, February 15, 2017, www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf
8. Jason Healey, "Beyond data breaches: global interconnections of cyber risk," Risk Nexus Report, Zurich Insurance Group and Atlantic Council, April 2014, www.zurich.com/_/media/dbe/corporate/docs/whitepapers/risk-nexus-beyond-data-breaches-global-interconnections-of-cyber-risk-2014.pdf?la=en&hash=64D3ABD783EDBDF227F5A696A3C1C086F52B132D. An analogy can be made with credit risks prior to the 2007-2008 financial crisis. Companies may have sold off their exposure to sub-prime mortgages, but those risks were still pooling elsewhere in the systems, largely unseen. Companies (and countries) that had no exposure to the initial risky mortgages were still critically affected by the cascading crisis.
9. The NIST Cybersecurity Framework is becoming the default standard. See the NIST website for the latest version (1.1) and additional information: www.nist.gov/cyberframework.

