THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

TECHNOLOGY

The ties that bind: A framework for assessing the linkage between cyber risks and financial stability

JASON HEALEY | PATRICIA MOSSER
KATHERYN ROSEN | ALEXANDER WORTMAN

20
YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

OPERATIONS

TECHNOLOGY

MILITARY

DEAR READER,

Welcome to this landmark 20th anniversary edition of the Capco Institute Journal of Financial Transformation.

Launched in 2001, the Journal has followed and supported the transformative journey of the financial services industry over the first 20 years of this millennium – years that have seen significant and progressive shifts in the global economy, ecosystem, consumer behavior and society as a whole.

True to its mission of advancing the field of applied finance, the Journal has featured papers from over 25 Nobel Laureates and over 500 senior financial executives, regulators and distinguished academics, providing insight and thought leadership around a wealth of topics affecting financial services organizations.

I am hugely proud to celebrate this 20th anniversary with the 53rd edition of this Journal, focused on 'Operational Resilience'.

There has never been a more relevant time to focus on the theme of resilience which has become an organizational and regulatory priority. No organization has been left untouched by the events of the past couple of years including the global pandemic. We have seen that operational resilience needs to consider issues far beyond traditional business continuity planning and disaster recovery.

Also, the increasing pace of digitalization, the complexity and interconnectedness of the financial services industry, and the sophistication of cybercrime have made operational disruption more likely and the potential consequences more severe.

The papers in this edition highlight the importance of this topic and include lessons from the military, as well as technology perspectives. As ever, you can expect the highest caliber of research and practical guidance from our distinguished contributors. I hope that these contributions will catalyze your own thinking around how to build the resilience needed to operate in these challenging and disruptive times.

Thank you to all our contributors, in this edition and over the past 20 years, and thank you, our readership, for your continued support!

Lance Levy, **Capco CEO**

THE TIES THAT BIND: A FRAMEWORK FOR ASSESSING THE LINKAGE BETWEEN CYBER RISKS AND FINANCIAL STABILITY

JASON HEALEY | Senior Research Scholar, School of International and Public Affairs, Columbia University, and Non-Resident Senior Fellow, Cyber Statecraft Initiative, Atlantic Council

PATRICIA MOSSER | Senior Research Scholar and Director of the MPA in Economic Policy Management, School of International and Public Affairs, Columbia University

KATHERYN ROSEN | Global Head, Technology and Cybersecurity Supervision, Policy and Partnerships, JPMorgan Chase

ALEXANDER WORTMAN | Senior Consultant, Cyber Security Services Practice, KPMG

ABSTRACT

Recent events have made clear that both the financial system and the networks of cyberspace are inherently complex, fragile, and interdependent. This paper contributes to the growing literature on cyber risks to the financial system by presenting a high-level analytical framework to guide analysis of how a cyber attack could cause financial instability and how financial system fragilities might be targeted by cyber attackers. The framework outlines linkages between the two sectors, particularly those which might cause contagion across the financial system. If a firm or market wants to understand systemic cyber risks in the financial sector, then conducting integrated analysis of how the various systems (technology, back office, business, and financial decisions) interact and propagate shocks collectively is key.

The paper is divided into four main sections: cyber risks, financial stability, the "transmission channels" by which cyber risks can induce financial turmoil, and the amplifiers and dampeners that shift the balance of risks. An appendix provides a sample set of questions designed to assist with implementation of the framework for a specific market, financial infrastructure or sector.

1. INTRODUCTION

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 attacks 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 cyberspace – are not just interconnected but interdependent. The modern financial industry cannot work without a functioning internet just as the organizations that keep the internet secure need the financial sector to be strong. Fortunately, research on cyber risks to financial stability has grown significantly in recent years, as we summarized in a previous article [Healey et al. (2018)].[1]

This 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 (DDoS), might initiate an episode of financial instability, or the reverse, how vulnerabilities in a particular part of the financial system (say, the payments system) might be targeted by

[1] You can also see the webcast of the launch event at the Atlantic Council: https://bit.ly/3uLYeGu.

various kinds of cyber incidents. The analytical framework is high level, intended to guide discussions on the linkages between the two sectors, particularly those that might cause contagion across the financial system. If a firm or market wants to truly understand systemic cyber risks in the financial services sector, then conducting integrated analysis of how the various systems (technology, back office, business, and financial decisions) interact and propagate shocks collectively is key.

This paper, which expands upon Healey et al. (2018), begins with a short section on financial stability and how cyber risks differ from the risks normally faced by the sector. We then provide an overview of the general framework through four main sections: cyber risks, financial stability, the "transmission channels" by which cyber risks can induce financial turmoil, and the amplifiers and dampeners that shift the balance of risks. The Appendix provides a set of questions to establish a baseline understanding of a particular market and to probe further each component of the framework as it relates to that market, as well as a series of institutions and papers that have contributed to the analysis of cyber risks to financial stability.

2. UNDERSTANDING FINANCE AND CYBER

The financial system performs various functions critical to the functioning of the broader economy, such as facilitating payment and settlement, allocating credit, transferring risk, and providing liquidity. As significant impairment of any of these core functions can cause instability, 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 that 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, rather than malice. A trader trying to corner the market or individual savers withdrawing money from a troubled bank are not out to 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 a malicious adversary to target vulnerable areas of the financial system in order to deliberately initiate financial instability or give a push to an economy teetering on the edge of collapse, to initiate or extend a crisis.

Fortunately, as expressed by Kevin Stiroh, then-Executive Vice President of the Financial Institution Supervision Group of the Federal Reserve Bank of New York [Stiroh (2019)], "resiliency to a cyber event is an area where the incentives of the private and public sector are closely aligned. Microprudential and macroprudential objectives are reinforcing." These alignments help not only to respond to cyber risks but to understand their impact to financial stability.

3. FRAMEWORK ON CYBER RISKS TO FINANCIAL STABILITY

The remainder of this 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. It is designed to be repeatable and adaptive, as well as market and technology agnostic.

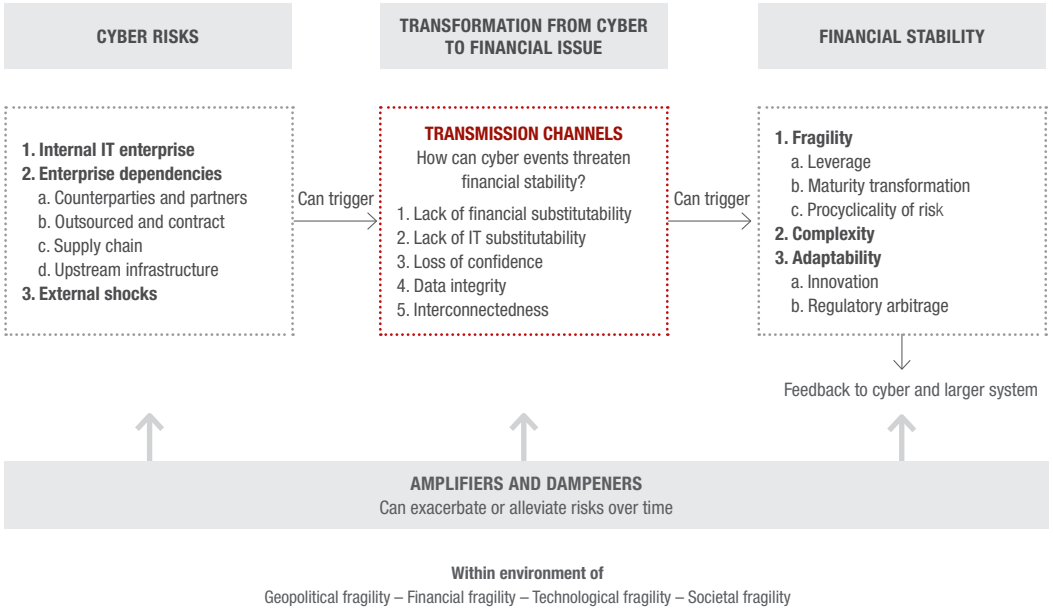
Figure 1 illustrates the basic framework, with risks flowing from left to right. Cyber risks can stem from one of several "aggregations" (on the left) that can then trigger a financial stability episode (right) through the transmission channels (center). Each category is affected by amplifiers and dampeners that can exacerbate or alleviate impact, all within an environment of inherent fragilities (bottom).

The cyber risks from the left side can, through the central 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, a sustained outage at a major cloud service provider would be a vendor-availability issue that may affect financial stability primarily through the lack of IT substitutability (but perhaps also confidence and interconnectedness).

The actual financial stability impact will depend on the resilience plans, proactive controls, and business and technology decisions taken in response to the attack as well

Figure 1: Cyber risks to financial stability – general framework



as the spillover effects those decisions have on other markets and firms. Under stable market conditions, even a massive cyber disruption may not cause financial instability. But if markets or the economy are particularly fragile (for example, if leverage is high and asset prices are falling) or if the attacker chose a uniquely vulnerable target at a specific moment, even a relatively modest incident might have a widespread impact on the financial system.

To use a real-world example, over the course of 2020, teams (most likely part of Russian intelligence) conducted an intrusion into SolarWinds, placing a Trojan horse into that company's popular network management software that was then downloaded by 18,000 other enterprises, including banks and the U.S. Department of the Treasury [Sanger et al. (2021)]. Despite being one of the most severe cybersecurity incidents in history, this supply chain incident did not have any systemic financial impact because the Russian motivation seems to have been the quiet collection of geopolitical intelligence rather than criminal theft from banks (as the North Koreans did against the Bank of Bangladesh) or widespread disruption of U.S. financial institutions, as the Iranians tried nearly a decade ago [Hammer (2018)].

To assess how a particular aspect of the financial system might be affected by a 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 (a lack of financial and IT substitutability). Research questions might include what cyber risks might have a large direct impact on the triparty market, which types of cyber attacks would be most likely to cause contagion and a destabilizing pullback in funding, or how a hostile adversary could time a cyber incident to trigger or exacerbate financial vulnerabilities in this market. These questions can be used to analyze any critical market or its infrastructure by examining the appropriate financial transmission channels and then extrapolating the cyber incidents most likely to disrupt those channels.

To assess the impact of amplifiers and dampeners to the financial 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?

4. FINANCIAL STABILITY RISKS AND VULNERABILITIES[2]

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

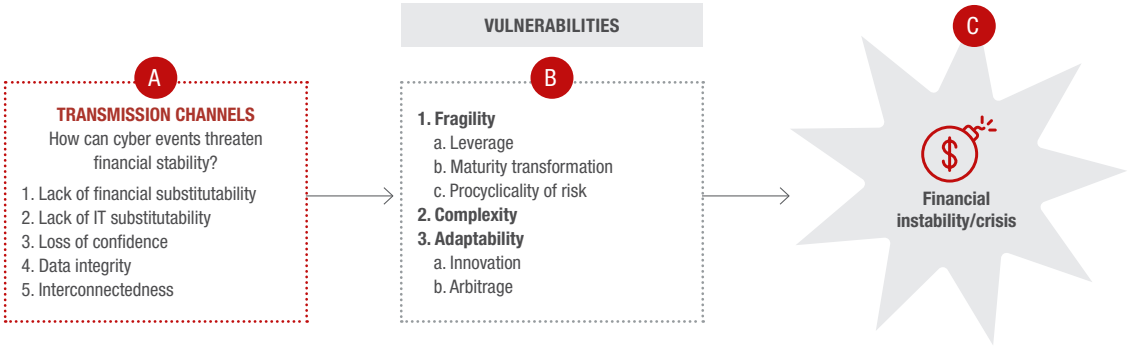
Fragility is one of the most important concepts in financial stability and includes three core characteristics of financial systems that contribute to systemic vulnerability: leverage, maturity transformation, and the procyclicality of risk. Leverage refers to being highly indebted at the level of the 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 in turn 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 complex web of financial markets, contracts, and institutions that allow shocks to propagate through the financial system, impacting sectors and activities that are not directly tied to the original shock. The business and behavioral reactions to negative shocks in particular tend to spill over rapidly (through trading, borrowing, and lending) from one firm or market to others in ways that are opaque and sometimes difficult to understand or model. This 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 through regulatory arbitrage. Innovation is the ability for market participants to push the envelope with new products, markets, and institutions that can be beneficial but can also increase the chances of mismeasuring new risks and thus a crisis. Innovations in some mortgage securitizations and related derivatives in the 2000s are notorious examples. Often innovation deliberately finds

Figure 2: Financial stability



Cyber risks transmitted through leftmost block (A) into traditional financial vulnerabilities (B), potentially causing financial instability or crisis (C)

[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.

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.

5. 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 that slices the risks by "aggregations", where the risks may pool far outside the enterprise [Healey (2014)]. 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.[3] 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 [Sandman (2014)].

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.

5.1 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 that 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.

5.1.1 INTERNAL IT ENTERPRISE

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. Industry best practices and regulations pave the way for established governance and controls.

5.1.2 ENTERPRISE DEPENDENCIES

Enterprise dependencies are just as important, however much they are overlooked by many enterprises. They include a growing array of third parties, utilities, and infrastructure providers an organization relies upon to conduct its business-critical and administrative 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 the exposure from contractual relations with external suppliers such as for human resources, legal, data, or IT support. **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, as seen in the Russian intrusions into SolarWinds and subsequent tampering of its software, widely used in the financial services sector. **Upstream infrastructure** is the risk from disruptions to infrastructure relied on by economies and societies, especially electricity, finance, and telecoms.

5.1.3 EXTERNAL SHOCKS

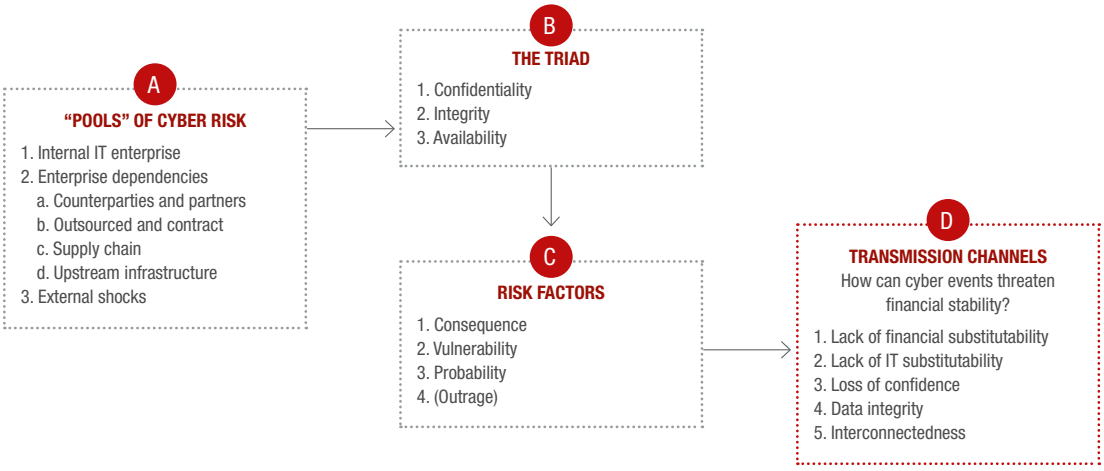
The third category of risks included in this model are those from incidents outside the system, outside of the control of most organizations and which are especially likely to cascade. Major international conflicts or malware outbreaks can cause or aggravate existing risks. The COVID pandemic has been such a shock, as is climate change and, increasingly, data-localization laws and the growing divergence between U.S. and Chinese technology ecosystems. Sudden erosion in any of these areas may be experienced as a cascading shock impacting cybersecurity to the finance sector.

5.2 The "triad"

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**

[3] Definitions for confidentiality/integrity/availability and consequence/vulnerability/probability are derived from NIST [Niels et al. (2017)].

Figure 3: Cyber risks (many ways to slice…)



Cyber risks (A) can be analyzed with "information security triad" (B). Each has unique equation of risk (C) making them more or less likely to be transmitted to the finance sector (D)

is preserving timely and dependable access and use of information against internet service provider (ISP) outages or DDoS attacks.

5.3 Risk factors

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 [Sandman (2014)].

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 of cyber risk and financial vulnerabilities. These channels can cause feedback loops to accelerate or dampen instability. To varying degrees, the likelihood and 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 sustained cloud outage or trading posture in an environment of corrupted or compromised data.

In 2017, The U.S. 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 [OFR (2017)]. The Cyber Risk to Financial Stability (CRFS) Project at the School of International and Public Affairs (SIPA) of Columbia University has added 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 that cannot be easily replaced. These are single points of failure for markets as they provide irreplaceable functions, such as payment systems, central counterparties, custodial and clearing bank services, exchanges and electronic trading platforms, and repo platforms (GCF, triparty).

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 and storage), key functions (such as internet exchange points and submarine cables), and even key communications protocols (like BGP).

3. **Loss of confidence:** it is difficult to predict the point where market participants lose confidence in a market, an infrastructure, or 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 infrastructure, and so decide to stop participating/transacting. This is particularly dangerous for short-term financing markets, because it can cause 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 in the U.S. Treasury securities market is an example of these two systems becoming further intertwined in a market critical to financial stability and the economy. A recent paper from the European Systemic Risk Board (ESRB) discusses how interconnectedness of the financial system, both operational and financial, can propagate cyber shocks across the system [Ros (2020)].

7. AMPLIFIERS AND DAMPENERS OF TRANSMISSION

The framework emphasizes amplifiers and dampeners as key components for any analysis of risks and contagion. Table 1 provides a few examples of such amplifiers and dampeners. 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 create a positive feedback loop or behave procyclically, which can magnify their impact and create systemic instability quite quickly.

These dynamics aid analysis in three ways: bottom-up assessments of how any amplifier or dampener, or set of these forces, may affect the entire system of cyber risk to financial stability, whether cyber risk, financial stability, or transmission factor; evaluations of any particular set of cyber risks (such as a major sustained outage at a cloud service provider (left-to-right analysis) or disruption to the triparty repo market (right-to-left); or understanding how changes to an amplifier or dampener are trends that will affect the system over time.

Some of the amplifiers and dampeners will be particular to individual technologies, firms, markets, and businesses. Others 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.

Some amplifiers and dampeners are relatively straightforward, such as mitigation for DDoS attacks, which removes the risks of disruption especially for large and capable financial institutions. Similarly, on the financial side, structural factors such as additional leverage and maturity transformation increase financial fragility amplifying the risk.

Other dynamics play out in complex ways that will be hard to unpack. Distributed ledgers and cryptocurrencies, for example, amplify some risks (such as bypassing regulatory structures and easing the monetization of cyber crime) while dampening them in others (like potentially reducing single points of failure). Likewise, the trends towards cloud computing and storage can increase concentration and vendor risks but reduce nearly every other risk. Similarly, additional capital required by regulators can make the financial system more robust to shocks in general, but capital standards based on short-run statistical measures can make risk management more procyclical, amplifying shocks.

Similarly, some types of financial products, for example some insurance products and credit default swaps, are hard to characterize. They may be amplifiers under some conditions and dampeners in others, depending on the state of the financial system, the cyber ecosystem, and the type of the shock.

Table 1: Examples of amplifiers and dampeners

	CYBER			FINANCIAL		
	TECHNOLOGY	OPERATIONAL	POLICY	STRUCTURAL	BEHAVIORAL	POLICY
AMPLIFIERS	• Increased IT complexity and dependence • Increasing number of endpoints • Single points of IT failure • Cloud computing (increases concentration and vendor risks) • Distributed ledgers and cryptocurrencies	• Data localization requirements • Diversified cyber crime markets • Miscalculation of residual risk	• Decreased international cooperation and governance • Increase in nation-state attacks • Growing alliance between nation-states and cyber criminals • Fragmented and conflicting regulatory environment	• Leverage • Maturity transformation • Single points of failure (market infrastructure)	• Procyclicality of risk (herd mentality) • Short-run statistical risk measurement and modeling • Variation margin	• Regulatory arbitrage • Statistical risk-based capital standards • Fair value accounting • Regulatory fragmentation
DAMPENERS	• End-to-end encryption • DDoS mitigation • Tokenization • Cloud computing (decreases most other cyber risks) • IT hardening standards and modern software methods like DEVSECOPS • Enterprise cyber defense suites and architectures	• Financial sector collaboration for analysis and information sharing • Cyber risk ratings and insurance • Cyber frameworks (NIST, Financial Sector Profile, global standards) • Cyber Kill Chain, ATT&CK, and other frameworks • Resiliency planning	• International treaties (Budapest Convention) • International norms for cyber conflict • Government support and information sharing with critical infrastructure • Regulatory harmonization • National risk registers	• Government back-stops and rescue package • Risk limits • Circuit breakers • Distributed ledgers • Disclosure and transparency standards	• Arbitrage ("buy low, sell high") incentives that balance crashes and booms • Initial margin	• Countercyclical capital regulation • Lender of last resort/deposit insurance • Activity restrictions • Third party vendor regulatory compliance • Liquidity requirements • Recovery and resolution planning

8. CONCLUSION

Cyber threats are considered one of the more important risks faced by financial companies – both large and small – and in particular, the financial system is uniquely vulnerable to system-wide disruptions due to the highly interconnected nature of both technology and financial businesses. Consequently, an integrated analysis of cyber risks and their transmission – through both technology and financial channels – is key to understanding how cyber attacks in specific financial markets or institutions could cause cascading impacts across the entire financial system. This paper has provided a framework for how private firms, the financial services industry, and the public sector can tackle this very complicated challenge, including an analysis of factors that can both amplify and dampen shocks. Importantly, our analytical framework is designed to assess how specific cyber attacks might be transmitted across the financial services sector, and in reverse how financial vulnerabilities might be exploited intentionally by cyber attackers.

APPENDIX A

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. If a firm or market wants to truly understand systemic cyber risks in the financial sector, then conducting integrated analysis of how the various systems – technology, back office, business and financial decisions – propagate shocks individually and how they interact with each other is key.

A.1 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 are 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?

A.2 Financial stability risks and vulnerabilities

Financial stability analysis typically focuses on key characteristics that 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 versus 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 various participants (intermediaries, investors, borrowers, lenders)?
   f. What are the key business decisions and who makes them when risk limits are breached?
   g. To what degree is herd mentality represented in the market?

2. Complexity

   a. How many steps are required for a typical trade – from pre-trade to 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 those 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?

A.3 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 that may pool far outside the enterprise [Healey (2014)].[4] Each has example questions drawn, where applicable, from the NIST Cyber Security Framework.[5]

[4] 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.

[5] The NIST Cybersecurity Framework is becoming the default standard. See the NIST website for the latest version (1.1) and additional information: https://www.nist.gov/cyberframework.

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 administered 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. Enterprise 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, pandemic, or a global economic crisis?

A.4 Principles

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?

A.5 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?

A.6 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 the 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 technology spillover effects of (various) cyber attacks? What are the financial spillover effects? Do those spillovers intersect?
f. What are the cross-border considerations with respect to risk management, regulation, data access, and IT standards?

A.7 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. As noted earlier, some features may be dampeners in some states of the world, but amplifiers in other states. 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 of sovereignty in cyberspace (analogous in many ways to ring-fencing financial institutions)?
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?
6. What are the trade-offs in the sector from cloud adoption between increased cybersecurity and increased concentration and vendor risks?
7. What is the impact from the broad trend of decreasing international cooperation and governance?

APPENDIX B: REFERENCES

Below is a list of institutions that have analyzed cyber risks to financial stability through policy papers and research papers.

The **Basel Committee on Banking Supervision (BCBS)**, a committee of banking supervisory authorities, issued "Cyber-resilience: range of practices" in 2018,[6] which compares bank, regulatory, and supervisory cyber-resilience practices across jurisdictions as well as details key metrics to measure cyber-resilience activities.

The **Bank of England** published its CBEST security assessment framework in 2014, designed to strengthen the cyber resilience of financial firms and financial market infrastructures by targeting participants' "crown jewels" in order to mimic and test defensive capabilities under cyber attack. In its 2018 "Financial Stability Report,"[7] the Bank of England stresses the importance of setting a baseline for cyber resilience as well as recovery times to mitigate cyber risks to the financial stability of the U.K.

The **Bank for International Settlements (BIS)**, the "central bank for central banks," issued "Regulatory approaches to enhance banks' cybersecurity frameworks" in 2017,[8] detailing specific regulatory and supervisory initiatives on cyber risk in four jurisdictions: Hong Kong, Singapore, the United Kingdom, and the United States. Recently, BIS research staff have published several studies on cyber risk in finance including: "Drivers of cyber risk" and "COVID-19 and cyber risk in the financial sector."[9] The BIS hosts numerous international standard setting bodies, including the Basel Committee on Banking Supervision.

The **Carnegie Endowment for International Peace,** the think tank in Washington D.C., published "International strategy to better protect the financial system against cyber threats," in 2020.[10] The paper is the work of the FinCyber Project and advocates for strengthening operational cyber resilience as the foundation for a comprehensive strategy to secure the global financial system. It focuses on seven elements for improvement: regulatory harmonization, response capabilities, data integrity, protecting single points of failure (such as FMIs), cost/benefit of cloud migration (concentration risk), information sharing, and defending against malicious intent.

The **Cyber Infrastructure & Security Agency (CISA)**, is a U.S. Federal Agency and part of the Department of Homeland Security tasked with understanding and managing cyber and physical risk to critical infrastructure within the United States. CISA's National Risk Management Center (NRMC) leads its effort in both evaluating and managing risks throughout the 16 critical infrastructure sectors and in 2021, announced the "Systemic cyber risk reduction venture"[11] to identify and reduce systemic cyber risk, particularly focusing on concentrated sources of risk. The initiative aims to achieve three goals: build the underlying architecture for cyber risk analysis to critical infrastructure, develop a cyber risk metric, and promote tools to address concentrated sources of risk.

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.[12]

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,[13] highlighting the unique characteristics and threats of cyber risk to FMIs.

The **European Banking Authority (EBA),** an E.U. regulatory agency mandated to assess risks to the E.U. banking sector and promote the harmonization of prudential rules, published "Policy advice on the Basel III reforms: operational risk," in 2019.[14] It recommended that ICT risk be incorporated into Capital Requirements Regulation (CRR) and Capital Requirements Directive (CRD) in order to improve assessments of operational risk.

[6] https://bit.ly/3bmaQwo
[7] https://bit.ly/2NZODvc
[8] https://bit.ly/2PyR1sZ
[9] https://bit.ly/3sSwazl; https://bit.ly/3ehB5Wq
[10] https://bit.ly/38ebl9H
[11] https://bit.ly/38d4hKm
[12] https://brook.gs/3v0l0cE
[13] https://bit.ly/38cCJVm
[14] https://bit.ly/3qnh3ML

The **European Systemic Risk Board (ESRB)**, an independent body responsible for mitigating systemic risk in the E.U. financial system, authored "Systemic Cyber Risk" in February 2020,[15] detailing an analytical framework to assess how cyber risk can become a source of systemic risk to the financial system. The four phases of the conceptual model (context, shock, amplification, and systemic event) demonstrate how a cyber incident can morph from operational disruption into a systemic crisis. In May 2020, the ESRB published "The making of a cyber crash: a conceptual model for systemic risk in the financial sector,"[16] exploring each phase of the conceptual model and elaborating on the individual variables at play. The paper concludes that a systemic event arising from a cyber incident is conceivable and that cyber incidents with near-systemic consequences have already occurred, yet a truly systemic event would require an assortment of amplifiers as well as a failure in systemic mitigants.

The **Federal Reserve Bank of New York (FRBNY)**, issued in 2020, "Cyber risk and the U.S. financial system: a pre-mortem analysis,"[17] in which it concludes that an adverse impairment, stemming from a cyber risk, of one of the five most active financial institutions could pose systemic risk.

The **Financial Stability Board (FSB)**, an international body created by the G-20 after the 2008 financial crisis to monitor the global financial system, created a "Cyber lexicon consultative document"[18] in 2018 for a common lexicon to foster better understanding of relevant cyber terminology and facilitate financial stability risk management practices. In 2020, the FSB conducted a series of expert workshops and public consultations examining cyber incident response and recovery, resulting in a best-practice report, which lays out a toolkit of more than four dozen practices that enhance firms ability to respond and recovery from cyber incidents: "Effective practices for cyber incident response and recovery: final report"[19]

The **Financial Stability Oversight Council** (FSOC), a U.S. federal government organization created in 2010 to monitor excessive risk to the U.S. financial system, has been analyzing cybersecurity as a primary risk to financial stability since 2012. In its "Annual report 2020",[20] the FSOC stressed that, "greater reliance on technology, particularly across a broader array of interconnected platforms, increases the risk that a cybersecurity incident may have severe consequences for financial institutions."

The **Institute of International Finance** (IIF), a global financial services trade association, issued "Cyber security and financial stability: how cyber attacks could materially impact the global financial system" in 2017,[21] 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,[22] emphasizing how cyber risks are unique and providing specific recommendations for effective regulatory policy. In "Cyber risk and financial stability: it's a small world after all," published in 2020, [23] the IMF notes that many national financial systems are not ready to manage attacks, arguing that mapping key financial and technology interconnections (cyber mapping) will aid in understanding and analyzing cyber risk to the financial system.

The **Office of Financial Research**, U.S. Treasury Department, has cited cyber as a financial stability risk in several recent reports. The OFR promotes financial stability by looking across the financial system to measure and analyze risks, perform essential research, and collect and standardize financial data.

[15] https://bit.ly/3rn65bk
[16] https://bit.ly/30gcb14
[17] https://nyfed.org/2MS2EdN
[18] https://bit.ly/3rmBXg1
[19] https://bit.ly/3sUWhFI
[20] https://bit.ly/30j7kwo
[21] https://bit.ly/38hSgn8
[22] https://bit.ly/2MR8aND
[23] https://bit.ly/2MR8cVL

The **World Economic Forum (WEF)**, an international organization centered on public-private cooperation, wrote in 2016, "Understanding cyber risk,"[24] acknowledging the complex interdependencies of financial networks, its increasing reliance on information technologies to operate, and the systemic risk posed by the potential consequences of an attack on systemically important institutions. In "Future series: cybersecurity, emerging technology and systemic risk," published in 2020,[25] WEF further explores the hidden and systemic risk posed by the increasing homogeneity of shared technologies and advocates for policy interventions to promote collaboration and accountability to identify and secure critical shared infrastructures and their key dependencies.

REFERENCES

Hammer, J., 2018, "The billion-dollar bank job," New York Times Magazine, May 3, https://nyti.ms/3pXDuI9

Healey, J., 2014, "Beyond data breaches: global interconnections of cyber risk," Risk Nexus Report, Zurich Insurance Group and Atlantic Council, April, https://bit.ly/3aZOVLg

Healey, J., P. Mosser, K. Rosen, and A. Tache, 2018, "The future of financial stability and cyber risk," Brookings, 10 October, https://brook.gs/3q544ze

OFR, 2017, "Cybersecurity and financial stability: risks and resilience," viewpoint, Office of Financial Research, February 15, https://bit.ly/2ZSOVq3

Niels, M., K. Dempsey, and V. Y. Pillitteri, 2017, "An introduction to information security," NIST Special Publication 800-12: Revision 1, June 2017, https://bit.ly/3dMygMV

Ros, G., 2020, "The making of a cyber crash: a conceptual model for systemic risk in the financial sector," European Systemic Risk Board Occasional Paper No. 16, May, https://bit.ly/37QLAw6

Sandman, P., 2014, "Introduction to risk communication and orientation to this website," 2014, https://bit.ly/3uCVL0Y

Sanger, D. E., N. Perlroth, and J. E. Barnes, 2021, "As understanding of Russian hacking grows, so does alarm," New York Times, January 2, https://nyti.ms/3dPCIdL

Stiroh, K., 2019, "Thoughts on cybersecurity from a supervisory perspective," SIPA's Cyber Risk to Financial Stability: State-of-the-Field Conference 2019, Federal Reserve Bank of New York, New York City, April 12, https://bit.ly/37NJLj9

[24] https://bit.ly/38cDQo0
[25] https://bit.ly/3rsSsHO

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO