BROOKINGS
Cybersecurity Project

THE BROOKINGS INSTITUTION | October 2018

The Future of Financial Stability and Cyber Risk

Jason Healey
Patricia Mosser
Katheryn Rosen
Adriana Tache

School of International and Public Affairs, Columbia University

Contents

STATEMENT OF INDEPENDENCE

The authors did not receive financial support from any firm or person for this article or from any firm or person with a financial or political interest in this article. Adriana Tache is a Vice President at the Fraud Fusion Center at Citi. Beyond that affiliation, the authors are not currently an officer, director, or board member of any organization with an interest in this article.

ABSTRACT

Cyber risks pose unique threats to financial stability that are not well understood or managed, despite growing investment in research and dependence by financial institutions, consumers, and governments on cyber technologies. This paper considers the ways in which cyber risks differ from traditional financial shocks. In contrast to the financial and policy shocks that have triggered past financial panics, cyber attacks are generally designed and initiated by sentient adversaries in aggressive pursuit of specific malicious goals. If one of those goals is broad financial system instability, a cyber attack may pose unique challenges.

Unfortunately, the interactions between the financial contagion channels and the technological and operational risk channels of cyber attacks have not been examined carefully. For example, a sustained attack on a large global financial institution could be contagious across both dimensions, but where and how the contagion channels might feed on each other and accelerate risk is an important area for future work. This paper starts by examining traditional risks to financial stability, such as contagion from excessive leverage. It also examines the current regulatory frameworks and partnerships, both domestic and international, established to increase the resilience of the financial system to cyber risk. The analysis concludes with major concerns and potential gaps in understanding and mitigating cyber risks to financial stability.

Introduction

The financial sector has long been at the forefront of cybersecurity and industry-wide information sharing and cooperation. Even so, cyber attacks on financial institutions and financial market infrastructures have become more frequent and sophisticated, prompting ever-larger security investments and increased focus on mitigating and managing cyber risk. Parallel to these efforts, the financial sector, regulators, and national governments have been working to improve overall resiliency and stability in the hopes of preventing a repeat of panics such as the financial crisis a decade ago.

This paper takes the critical next step: examining the intersection of these two efforts. How might cyber risks and financial risks interact to cause systemic crises? Is there anything fundamentally new or different about cyber risks? How should economists, regulators, policymakers, and central bankers focused on financial stability incorporate cyber risks into their models and thinking?

Some of the most direct initiatives on these questions began in 2013, after a White House Executive Order instructed the Department of Homeland Security, in consultation with the Department of Treasury, to identify those financial institutions for which "a cyber incident would have far reaching impact on regional or national economic security."[1] In response, eight leading financial institutions created the Financial Systemic Analysis & Resilience Center (FSARC) in 2016, concentrating sector efforts on "*systemic risk* to the U.S. financial system from current and emerging cyber security threats."[2]

Over the past two years, Columbia University's School of International and Public Affairs has hosted a series of engagements bringing together industry experts from the FSARC and its member institutions, regulators and other policymakers, and academics with backgrounds in finance and cybersecurity.

This paper is the result of those efforts to better frame the issues and formulate additional steps to understand and mitigate the financial stability risks posed by cyber attacks. It begins with an analysis of traditional risks to financial stability and how they compare to cyber risks; continues with a survey of efforts to date to address these risks; and ends with recommendations.

. . .

1. Exec. Order No. 13636, 3 C.F.R. 13636 (2013).

2. FS-ISAC. (2016, October 24). FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC) [Press release]. Retrieved from http://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html. Emphasis added.

Traditional vulnerabilities that can trigger financial instability

There is no single comprehensive definition of "financial stability." In general, it refers to the ability of the financial system "to facilitate and enhance economic processes, manage risks, and absorb shocks."[3] Even in a stable financial system, asset prices and interest rates can be volatile, banks and financial companies can fail, investors can lose money, and borrowers can default.

Policymakers allow such failures, instead prioritizing stability, that is, the prevention and management of systemic cycles that could severely weaken or shut down the economy. The financial system performs various functions such as facilitating payments and settlements, allocating credit, transferring risk, and providing liquidity, as well as maturity transformation and price discovery. Significant impairment of any of these core functions can cause financial instability.

Financial stability authorities are, therefore, concerned with the ways in which financial markets and institutions can propagate and amplify shocks, regardless of their source. Of notable interest are the dynamics – also called vulnerabilities – that can lead to financial crises (e.g., runs on banks and wholesale funding markets, fire sales of assets, loss of confidence). Historically, these vulnerabilities have led to deep recessions or depressions, deflation, and long subsequent periods of subpar growth and unemployment.

Three features of the financial system can create vulnerability:

Leverage: Higher levels of leverage – that is, indebtedness – are linked to higher levels of systemic vulnerability. Those market participants, positions, and financial institutions with the highest leverage tend to generate the most contagion regardless of the nature of the shock. With high leverage, even a moderate decline in the value of assets can cause a sharp decline in financial institutions' equity and the ability to absorb loss to plummet, resulting in financial distress or insolvency.

Maturity and Risk Transformation: Financial systems transform longer-term, risky, illiquid assets (such as the now-infamous subprime mortgages) into safer, more liquid assets (most obviously, money itself). During this transformation process, a shock to the price of risky illiquid assets can lead to a withdrawal of funding and cause contagion by forcing asset sales and, in the extreme, the failure of core institutions and a systemic crisis.

Procyclicality of the price of risk: This procyclicality interacts with leverage and maturity transformation to magnify asset price booms and busts. For example, falling asset prices drive the value of the collateral of borrowers (i.e., their net worth) down and the cost of borrowing (risk premia and interest rates) up. By increasing the risk to lenders, this

. . .

3. Schinasi, Garry J. (2004). *Defining Financial Stability*. IMF Working Paper No. 04/187. Retrieved from http://www.imf.org/en/Publications/WP/Issues/2016/12/31/Defining-Financial-Stability-17740

dynamic depresses risky asset prices even further, creating a feedback loop of reduced funding, greater losses and higher risk premia.

These vulnerabilities, and particularly interactions between them, can leave financial systems fragile and subject to periodic crises and runs. The timing and specific triggers of crises are hard to predict. As a result, analysis of financial system stability typically focuses less on the shocks and triggers of crises, and more on identifying and dampening the vulnerabilities and propagation mechanisms that make the system unstable in the first place.

The triggers for past crises have mostly been shocks (often seemingly insignificant ones) instigated by financial market participants (e.g., lenders, investors) or by macroeconomic policy changes. This begs the question: how does cybersecurity risk affect financial stability?

What is different about cyber risk?

In 2016, the Office of Financial Research (OFR) of the U.S. Department of the Treasury wrote in its Financial Stability Report to Congress that the vulnerability of "cybersecurity incidents affecting financial firms" introduced specific risks to contagion as well as funding and liquidity.[4] In that report and a related research paper, the OFR highlights the three "channels" by which these risks could be transmitted, potentially leading to systemic crises[5]:

Lack of (Financial) Substitutability: The financial system depends on a few key hubs, typically certain firms or utilities (e.g., electronic trading systems, exchanges, or clearing houses), that perform a vital function for the entire industry. Examples of these functions include custody of securities, collateral management, and trade matching and confirmation, all of which are technology-intensive, automated processes. In short, the "financial services industry relies on a robust Information and Communications Technology (ICT) infrastructure to complete transactions or move payments."[6] There would be little easy substitution workarounds if an incident were to affect these institutions or systems.

Loss of Confidence: The OFR notes that attacks routinely affect consumer networks with no systemic impact, but also that a "wider-reaching theft … could cause a broader loss of confidence."[7] It might not take a theft of customer data to trigger such a loss. A wide range

. . .

4. Office of Financial Research. (2016). *2016 Financial Stability Report*. Retrieved March 28, 2018, from https://www.financialresearch.gov/financial-stability-reports/files/OFR_2016_Financial-Stability-Report.pdf

5. U.S. Treasury Department Office of Financial Research. (2017). *Cybersecurity and Financial Stability: Risks and Resilience.* Retrieved from

6. U.S. Treasury Department Office of Financial Research. (2016). *2016 Financial Stability Report*. Retrieved from https://www.financialresearch.gov/financial-stability-reports/files/OFR_2016_Financial-Stability-Report.pdf

7. Ibid.

of attacks could do the trick: ATM hacks, takedowns of one or more particularly trusted institutions, hacker-induced flash crashes, releases of compromising emails from bankers or regulators, or account takeovers. Whatever the trigger, a sufficiently extreme loss of confidence could cause a "run on the banks."

Data Integrity: Systemic impacts could arise from cyber intrusions that directly modify or otherwise affect the quality of market or consumer data, causing the system to pause until any remaining uncorrupted backups can be restored. As many institutions have learned in recent ransomware attacks such as WannaCry, restoration can take longer than expected and cause loss of confidence or other systemic impacts, "particularly for markets that process orders rapidly."[8]

We believe that at least one channel should be added to the three identified by the OFR:

Lack of (ICT) Substitutability: OFR highlights that the finance sector depends on a few key hubs, but of course this is true of ICT as well. For example, a large (and growing) percent of the world's computing and storage falls to just a few cloud service providers; corporate IT enterprises tend to be extremely similar and run the same operating systems and applications; all companies depend on the same basic Internet protocols, like TCP/IP or DNS, and local disasters often reveal unexpected physical dependencies by disrupting entire regions or industries.

These "channels" are literally paths by which a cyber event could transform into a financial crisis. To understand how this can happen, we must identify the three main differences between cyber and financial shocks that can create systemic instability: timing, complexity, and adversary intent.

- **Timing of Attacks**: Typical triggers of financial instability – financial or policy shocks – can seem small and randomly timed. It is the outsized reaction of markets and financial firms to those shocks (through the contagion channels of leverage, etc.) that causes wide-spread damage. In contrast, cyber attacks require long-term planning. Adversaries infiltrate a system weeks or months beforehand to map it, elevate their privilege, and determine how best to cause disruption. The upside is that the attacks most likely to cause instability require a massive amount of preparation. The downside, however, is that once in place, the disruptions can be triggered at a time of the attacker's choosing.

- **Complexity**: Cyberspace is an incredibly complex system – complex at the physical, network, and cognitive levels. Because complex systems are highly interconnected and tightly coupled, disruptions in one area can cascade easily and in unexpected ways. This "unacknowledged correlated risk of cyberspace is why cyberspace is capable of black swan behavior," of very unpredictable, extremely

. . .

8. Ibid.

high-consequence events.[9] Of course, the financial sector is also complex and capable of black-swan behavior, but at least in finance this complexity is the object of intense study by risk specialists using advanced and mature models. These simply do not exist to the same degree for cyber risk. There is little understanding of the ways in which the failure, whether by accident or adversary design, of an IT company "too big to fail" (such as a major cloud service provider) might cascade.

- **Adversary Intent**: The third and most crucial key difference is that cyber risks are generally imposed and initiated by the willful actions of sentient adversaries in aggressive pursuit of specific malicious goals.

For traditional financial shocks, it is well understood that small behavioral changes on the part of the sector's participants or small policy changes can have disproportionately large impacts on stability if the system is in a fragile state. The risk of a small shock creating financial instability is particularly elevated when the level of leverage, the degree of maturity transformation, and the price of risky assets are high.

Although capable of causing widespread harm, traditional financial and macro-policy shocks tend to arise out of self-preservation 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, may be targeted and timed to disable, destroy, corrupt, or compromise market functioning, deliberately initiate financial instability.

So far, cyber adversaries have mostly been individuals or small groups out for quick profit, with little demonstrated interest in systemic impact. This may change as the gains and motivations for financial cyber crimes evolve. As one report noted in 2010,

> In the early years, cybercrime was clumsy, consisting mostly of extortion rackets that leveraged blunt computer network attacks against online casinos or pornography sites to extract funds from frustrated owners. Over time, it has become more sophisticated, more precise: like muggings morphing into rare art theft.[10]

Cyber attacks have become more sophisticated ("less smashy, more grabby"[11]) such as the 2017 targeted phishing campaign which was waged against "personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations,"

. . .

9. Geer, Jr., Dan. (2018). *A Rubicon*. Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1801. p. 1. Retrieved from https://www.hoover.org/sites/default/files/research/docs/geer_webreadypd-fupdated2.pdf.

10. Villeneuve, Nart. (2010). *Inside a Crimeware Network*. Infowar Monitor Technical Report No. JR04-2010 Retrieved from https://citizenlab.ca/wp-content/uploads/2017/05/koobface.pdf

11. Mandiant. (2017). *M-Trends 2017: A View from the Front Lines* [PDF File]. Retrieved March 28, 2018, from https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

in order to gain advance knowledge of filings to commit securities fraud.[12] Other examples include North Korean intrusions into the Bangladesh central bank to attempt to steal USD 951 million through the SWIFT global payment messaging system[13] and the attack on Banco de Chile, the country's largest bank, that "crashed over 9,000 computers and over 500 servers…to access the systems connected to the bank's local SWIFT network."[14]

These schemes depended on a functional financial system for the adversary groups to cash out, but still threatened significant systemic risk. Cyber criminals and nation-state attackers are targeting core financial infrastructure. They may not intend to instigate cascading failures, but even sophisticated adversaries can make mistakes, potentially sparking a crisis if the system is already fragile.

More importantly, some groups seem to be embracing what was once idle speculation and the plot of bad movies: the exploitation of cyber capabilities to induce financial instability. Iran, the most salient example, from 2011 to 2012 conducted a massive denial of service attack against nearly 50 major financial institutions not because "that's where the money is" to steal it, but apparently to generate a larger financial disruption.[15] If U.S. sanctions cut off a nation from the U.S. dollar market, that nation's leadership might decide it would have little to lose by causing significant disruptions to the financial system which might inflict grave damage to the economies of the United States and its allies.

Historical examples suggest that the most damaging cyber attacks are the work of the most capable and persistent (in the face of cyber defenses) attackers. A large disruption over a long period of time requires the capabilities of a large organization, up to and including the bureaucracy of a nation-state. Such attackers are also more likely to have the detailed resources and research necessary to understand complex financial markets, institutions, and network infrastructures, find and exploit vulnerabilities using tailor-built weapons, and determine the best timing for maximum disruption as part of, or in lieu of, a larger political or military goal.

. . .

12. Miller, Steve. (2017, March 7). *FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings.* Retrieved from www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html

13. Corkery, Michael, and Matthew Goldstein. (2017, March 23). *North Korea Said to be Target of Inquiry Over $81 Million Cyberheist.* The New York Times. Retrieved from www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html

14. Cimpanu, Catalin. (2018, June 8). *Hackers Crashed a Bank's Computers While Attempting a SWIFT Hack.* Bleeping Computer. Retrieved from https://www.bleepingcomputer.com/news/security/hackers-crashed-a-bank-s-computers-while-attempting-a-swift-hack/

15. According to the indictment from the U.S. Department of Justice, hackers associated with the Iranian Revolutionary Guards Corps directed a near-daily "onslaught of cyber-attacks on 46 of [the US's] largest financial institutions," according to an indictment of the U.S. Department of Justice. The attack was probably Iran's "retaliation for Western economic sanctions and for a series of cyberattacks on its own systems," including the Stuxnet attack on centrifuges involved in uranium enrichment. There seems little doubt of Iranian involvement, as one of the hackers even "received credit for his computer intrusion work from the Iranian government towards his completion of his mandatory military service requirement in Iran." U.S. Department of Justice. (2016, March 24). *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector* [Press release]. Retrieved from https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

Sparking Crises

Adversaries can cause three different types of crises: slow-burn, initiated, or exacerbated. Slow-Burn Crises occur when an adversary uses cyber capabilities to cause long-term friction, loss of confidence, and disruption, but below the level of "crisis" that might cause the nation under attack to respond militarily. Examples include Iran's DDoS attacks on U.S. financial institutions and North Korea's ongoing heists and disruptions (as noted above). These actions have thus far fallen short of triggering a systemic crisis.

Exacerbated Crises happen when a financial crisis is already in progress or a nation is teetering on the edge of one, and an adversary intentionally gives it a push with a cyber attack. Imagine the many ways a cyber attack could have further disrupted policy and market responses in 2008, when global central banks and domestic authorities were mounting massive liquidity and capital support to troubled financial institutions. DDoS attacks could have disrupted email or phone communications and interfered with central bank lending programs or FDIC bank resolution execution, inciting further panic and bank runs. Adversaries might have released sensitive (or doctored) emails to enrage citizens and legislators over a bailout; or ransomware attacks on distressed firms could have disrupted the due diligence needed to ensure they could be bought, closed or saved. In the midst of a fast-running bear market, cyber-induced flash crashes could tip global stock or bond markets into a rout.

Initiated Crises, the opposite of exacerbated crises, arise when an adversary uses cyber capabilities to create a financial crisis that would not otherwise have occurred. In order to inflict maximum economic damage, an attack on critical financial infrastructure – such as a payment or wholesale funding system – could hit at precisely the place and time that the infrastructure is most economically and technologically fragile. Attacks could target liquidity provision and funding markets, key collateral, settlement, and transaction systems and their associated vendor support systems, in addition to systemically important financial institutions or utilities and critical Internet infrastructure. The lack of substitutability creates a rich set of potential targets.

In short, cyber attacks differ from traditional financial and policy shocks in both intent and timing. While no attacks to date have resulted in financial instability, the potential impact of a carefully timed cyber attack designed to exploit the (negative) dynamics associated with traditional financial contagion channels has been insufficiently examined.

Existing work on cyber risk and financial stability

With the number and sophistication of cyber attacks on the rise, only collaboration among industry participants as well as private and public institutions, both domestically and internationally, can ensure resilience in the financial system.

Early Efforts

The attacks of 11 September 2001 prompted a sense of urgency in predicting and stopping future threats. Digital infrastructure and cybersecurity became top priorities in the United States. The Financial Services Information Sharing and Analysis Center (FS-ISAC), established voluntarily several years earlier in response to a White House request, took on added responsibility to coordinate sector responses to incidents such as major malware and worm attacks, including Nimda and SQL Slammer (and the Iranian DDoS attacks on the financial sector a decade later). The sector created parallel organizations for higher-level incident response and policy coordination. The private-sector Financial Services Sector Coordinating Council (FSSCC) was created in 2002 with seventy of the "largest financial institutions and their industry associations representing banking, insurance, credit card networks, credit unions, exchanges, financial utilities in payments, clearing and settlement."[16] With the engagement of senior-level leaders from around the sector, the FSSCC produces strategies and response plans for cyber and other homeland security risks, such as epidemics and terrorism.

The public sector cousin to the FSSCC is the Financial and Banking Information Infrastructure Committee (FBIIC), created (also in 2002) to "improve collaboration among financial regulators, improve financial sector resiliency, and promote a stronger partnership between the public-private sector."[17] The FBIIC and FSSCC meet quarterly, bringing members of both together to increase trust and improve responses across the public-private divide. The Treasury has funded important work in this area, including improvements to crucial financial infrastructure and a 2004 contract to the FS-ISAC to provide service to all U.S. financial institutions, not just members.

Among the most important specific systemic efforts was the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, issued in 2003 by the Federal Reserve Board, Office of the Comptroller of the Currency, and Securities and

. . .

16. Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. (2017, May 12). *Cyber Executive Order Strong Step Toward Enhancing National Security* [Press release]. Retrieved from https://www.fsscc.org/files/galleries/FSSCC_Cyber_EO_release_5_12_17.pdf

17. FBIIC. *Mission and History.* Retrieved from https://www.fbiic.gov/mission-history.html

Exchange Commission.[18] This joint policy established "sound practices to ensure the resilience of the U.S. financial system, which focus on minimizing the immediate systemic effects of a wide-scale disruption on critical financial markets," including from cyber means. This work dovetailed with that of the Basel Committee on Bank Supervision, which issued its initial Basel 2 regulations on operational risks the following year.

Acknowledgement of Cyber Risk as a Trigger of Financial Instability

More recently, international groups have begun recognizing the importance of cyber risks and developing policy responses. Other recent practical projects will be discussed in the next section.

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 guidelines for financial market utilities (FMIs) in 2012. In June 2016, it followed up with "Cyber guidelines for FMIs." This paper highlighted the "unique characteristics of cyber risk," including "the persistent nature of a campaign conducted by a motivated attacker" and the "broad range of entry points through which an FMI could be compromised." It also noted that "certain cyber attacks can render some risk management and business continuity arrangements ineffective," as when data backups propagate malicious software.[19]

At the highest levels, the G-20 has begun to focus on malicious use of ICT and its ability to endanger financial stability. The G-20 delegated to the Financial Stability Board (FSB) the task of performing "a stock-taking of existing relevant released regulations and supervisory practices in our jurisdictions, as well as of existing international guidance, including to identify effective practices" in cybersecurity. To this end, the FSB has conducted research and workshops, presenting its findings to G-20 leadership in October 2017. The FSB was also tasked with establishing a common lexicon to foster better understanding of relevant cyber terminology and facilitate financial stability risk management practices.[20] At the G-7 level, member countries came together to release the *G7's Fundamental Elements of Cybersecurity for the Financial Sector* in October 2016, offering eight elements to follow in designing and implementing a cybersecurity program. This was followed by a report setting out *The Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector* in October 2017. This report emphasized five key elements for cybersecurity program assessments and improvements.

. . .

18. U.S. Securities and Exchange Commission. (2003, April 7). *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System; Release No. 34-47638.* Retrieved from https://www.sec.gov/news/studies/34-47638.htm

19. CPMI-IOSCO. (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures*. Retrieved from https://www.bis.org/cpmi/publ/d146.pdf

20. Financial Stability Board. (2018). *Cyber Lexicon Consultative Document*. Retrieved from http://www.fsb.org/2018/07/cyber-lexicon-consultative-document/

In an unofficial 2017 working paper, the International Monetary Fund (IMF) listed, as we do in this paper, the ways in which cyber risks are unique. The IMF paper, however, offers more specific recommendations, especially for effective regulatory policy, suggesting that "cybersecurity risk needs to be managed using both ex-ante regulation and ex-post liability," "the regulatory architecture needs to adapt and be continually refined," and "high level principles should be complemented with bespoke guidance at the firm level."[21]

In August 2017, the BIS furthered thinking in this space by releasing a report on developments in four jurisdictions with "specific regulatory and supervisory initiatives on banks' cyber-risk; these include Hong Kong SAR, Singapore, the United Kingdom and the United States."[22]

In September 2017, the Institute of International Finance published an important paper emphasizing that "cyber-attacks do not stop at the border, and neither should the efforts aimed at responding to them."[23] With four scenarios of cyber risk transmission through the global financial system (see Text Box 1), IIF argues that cyber defense should be approached "holistically [and] considering all the actors involved, using the many technical and legal tools available, developing new ones if needed, and always seeking international cooperation and promoting harmonization" of regulation.

Text Box 1: IIF's Cyber Scenarios Which May Affect Financial Stability

1. A major "wholesale payment system and a large retail payment system attacked at the same time, so that neither can provide their services, for example, over a 24-hour period."
2. "Major data corruption at a custodian bank and one of the large Central Securities Depositories."
3. "Direct attacks on parts of the wider infrastructure that the financial system relies upon," such as the electrical grid.
4. "Retail consumers and broader society … distrust the safety and soundness of parts of the financial system [either] because of a few very significant cyber-attacks or many very frequent successful smaller attacks on financial institutions or on financial markets infrastructures."

In the United States, the Financial Stability Oversight Council (FSOC) (created in 2010 by the Dodd-Frank Act) has been analyzing cyber security as a primary risk to financial stability since 2012.[24] In 2017, the FSOC highlighted several practical solutions, including automated sharing of cybersecurity 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.[25]

. . .

21. Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson. (2017). Cyber Risk, Market Failures, and Financial Stability. IMF Working Paper WP/17/185. Retrieved from https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx

22. Bank for International Settlements, Financial Stability Institute. (2017). Regulatory Approaches to Enhance Banks' Cyber-Security Frameworks. Retrieved from http://www.asbasupervision.com/en/bibl/recommended-reading/1556-lr241/file

23. Boer, Martin, and Jaime Vazquez. (2017). Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System. Institute of International Finance, p. 9. Retrieved from www.iif.com/system/files/iif_cyber_financial_stability_paper_final_11_13_2017_clean.pdf

24. Financial Stability Oversight Committee Annual Report 2012, 2013, 2014, 2015, 2016 and 2017. Retrieved from https://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2017-Annual-Report.aspx

25. Financial Stability Oversight Council. (2017). 2017 Annual Report. Retrieved from https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC_2017_Annual_Report.pdf

Enhanced Protection and Resilience

In addition to these policy responses, there have been several specific efforts, especially in the United States, where DDoS attacks against many of the largest banks in 2012 hastened the need for enhanced cybersecurity protection and coordination between the public and private sectors.

In 2013, the White House issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, to drive cyber-related industry efforts. Section 9 of that policy ordered the Secretary of the Department of Homeland Security (DHS) to identify "critical infrastructures" that could affect "public health or safety, economic security, or national security" if they became the victims of cyber attacks.[26] DHS worked with the Treasury to determine which financial institutions and utilities fit this description. The resultant list of financial institutions is classified but will certainly overlap to some degree with those identified by the Dodd-Frank Act's systemically important financial institutions.

Eight of the "Section 9" banks decided, at the CEO level, to come together to create the Financial Systemic Analysis & Resilience Center (FSARC), now a subsidiary of the FS-ISAC. The founding members – Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street and Wells Fargo – created the FSARC to "proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats through focused operations and enhanced collaboration between participating firms, industry partners, and the U.S. Government."[27]

The FS-ISAC's "Sheltered Harbor" project resulted in financial industry associations and their members taking steps "to securely store and rapidly reconstitute account information, making it available to customers, whether through a service provider or another financial institution, if an institution appears unable to recover from a cyber incident in a timely fashion."[28] This data backup is not for recovery, but to guide deposit insurance in the event of resolution, the final death of the company. This creates a bulwark against loss of confidence in the event of a large number of bank failures with data corruption or destruction.

Cyber exercises in both the public and private sectors play an important role in identifying gaps and weak points for possible exploit. Sheltered Harbor was a direct result of les-

. . .

26. Office of the White House Press Secretary. (2013, February 12). Executive Order: Improving Critical Infrastructure Cybersecurity [Press release]. Retrieved from obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

27. FS-ISAC. (2016, October 24). FS-ISAC Announces the Formation of the Financial Systemic Analysis & Resilience Center (FSARC) [Press release]. Retrieved from http://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html

28. FS-ISAC. (2016). Sheltered Harbor Fact Sheet. Retrieved from www.fsisac.com/sites/default/files/news/SH_FACT_SHEET_2016_11_22_FINAL3.pdf

sons learned from cyber exercises. On average, major players in the banking industry subject themselves to one exercise simulating a different scenario every quarter.[29] For example, the FS-ISAC and the Payments Risk Council conduct yearly table-top exercises that simulate a cyber attack against payment processes (CAPP). According to the National Automated Clearance House Association (NACHA), these simulations help to identify gaps in incident response plans, strengthen incident response team relationships, build understanding of system vulnerabilities, and drive exploration of improvements in response.[30] There have been at least 19 events in the Hamilton Series of exercises (sponsored by the U.S. Department of Treasury). The Hamilton Series is a set of exercises developed by the FS-ISAC, FSSCC, Treasury Department, and other relevant US government agencies that simulates an assortment of cyber attacks or incidences in financial services in order to improve public and private sector policies, procedures and coordination. In 2015, the British and U.S. governments conducted a joint exercise with the private sector to improve understanding between government and industry for information sharing, incident response, and public communications.

Resiliency efforts to date have centered on the United States. However, in 2013 the FS-ISAC expanded its charter to include global financial institutions in regions such as Asia, Europe, and North and South America.

Major concerns and recommendations

Great progress has been made on cyber defense, both domestically and across borders. Exercises are being conducted, financial system processes are being mapped, and the weak links in networks can be detected. However, four major concerns linger:

Adversaries. Increasingly knowledgeable and sophisticated adversaries might deliberately aim for (or unintentionally cause) financial instability and actively work to undermine the financial sector's response efforts. The complexity of technological dependence has sparked a related and growing concern: that even unsophisticated actors might be able to trigger systemic effects.

Lack of Understanding. There is a dearth of information and analysis on the potential interactions of cyber risks, financial contagion channels, and possible "amplifiers" within those channels, such as single points of failure. Further work here is crucial for understanding how cyber risk intersects with business flows and decisions when markets and institutions are under stress.

Fragmentation of Efforts. There is a misalignment of cross-border policies, a divergence between industry and official sector work on cyber and financial stability risks, a lack of coordinated policies and regulations, and a range of standards and preparedness

. . .

29. Statement made April 18, 2017, by participant at SIPA "Cyber Risk and Financial Stability" workshop.

30. NACHA. Cyber Attack Against Payment Processes Exercise. Retrieved from https://www.nacha.org/events/cyber-attack-against-payment-processes-exercise-2017

across different types of firms and markets. Even though cyberspace, like the financial sector, is global and interconnected, responses to major crises remain significantly national. There are no organizations like the BIS, IMF, or G-20 in place to help coordinate international standards, communication, and responses to a systemic cyber event.

New Technologies. Even though the financial system is already highly complex, it will continue to betransformed, especially with the explosive growth of fintech. Some of these technologies will have a systemic impact; some will accelerate risk, and others will dampen it. For example, blockchain may dampen risk by reducing single points of failure, while cloud computing reduces most cyber risks but increases dependence on a few key providers. It will be especially difficult to develop controls in the face of increased financial and technological complexity.

Recommendations

Given these concerns, our recommendations emphasize greater shared understanding of the two disciplines – financial stability and cyber risk – and their intersections, as well as actions to harmonize approaches to resilience across the financial sector. These recommendations include:

1. Harmonize international regulations that foster resilience to cyber attacks and mitigate risk in the event of an attack. This regulatory and supervisory approach should have enough elasticity to evolve with technological changes and adversary sophistication.

2. Conduct additional research to identify data and facilitate the design of models to measure or quantify cyber risk, including the development of a shared lexicon or taxonomy to discuss cyber risk as a factor in financial stability. We are encouraged by the FSB's effort, initiated in July 2018, to create a lexicon for cyber security and cyber resilience through its Consultative process. However, we believe a lexicon should be *shared* between the cyber and financial stability communities, not just for the benefit of the financial experts, to foster greater two-way communication and resilience. For example, the lexicon omitted "risk" and "attack," which have different meanings in the cyber and financial stability communities and could lead to misunderstanding in the heat of a crisis.

3. Share and further develop maps of critical market structures, as well as market processes and conventions (both recent public and private sector efforts) and develop additional maps to better understand the overlay of cyber risk on the plumbing of markets and institutions. Particular focus should be given to how cyber technology contagion may interact with business decisions and financial responses, which in turn can induce financial contagion. Develop action plans based on this understanding and use of these maps.

4. Conduct more exercises, at the domestic level and cross-border, especially to bridge between senior-level response executives from the financial stability and cybersecurity communities. Stakeholders should include C-level executives from cybersecurity companies, regulators, banks, and central banks. Exercises should increasingly include all global financial centers and regulators to match the global nature of both cyberspace and finance.

Every year, cyber attacks become more severe and adversaries more daring. The global financial sector has been a target, not of mere criminal bank jobs or credit card theft, but far larger and more sophisticated attacks. These attacks might have had a systemic impact but for the heroic efforts of technologists and decision makers. Adversaries, by design or accident, will conduct someday an attack that is beyond the ability of these defenders to contain. It has never been more important to continue the work of reconciling and mitigating cyber risks to financial stability.

BROOKINGS

The Brookings Institution is a nonprofit public policy organization based in Washington, DC. Our mission is to conduct in-depth research that leads to new ideas for solving problems facing society at the local, national and global level.

Questions about the research? Email communications@brookings.edu.
Be sure to include the title of this paper in your inquiry.