Cybersecurity and Financial Stability

Loretta J. Mester
President and Chief Executive Officer
Federal Reserve Bank of Cleveland

2019 Financial Stability Conference
Financial Stability: Risks, Resilience, and Policy
Federal Reserve Bank of Cleveland and the Office of Financial Research
Cleveland, OH

November 21, 2019

Introduction

It is a pleasure to welcome you to the Federal Reserve Bank of Cleveland for what I expect to be a very engaging discussion of issues surrounding the stability of the financial system. I extend a special thanks to our partner, the Office of Financial Research (OFR), and Stacey Schreft, deputy director of research and analysis at the OFR. She and Joe Haubrich of the Cleveland Fed have worked diligently to put together this two-day program, the sixth joint conference between our two institutions. A look back at those past programs shows that much work has been done to increase our understanding of the risks facing the global financial system and the effectiveness of policies intended to foster increased resilience. Advances in research, data collection, and risk-monitoring have given us all a better appreciation of the interlinkages underlying the global financial system and the ability of a disturbance in one part of the system to propagate across the system. The horizontal approach to risk-monitoring, including stress testing, has been an important advance in the supervisory tool kit. Policymakers are gaining a better sense of how macroprudential policy and monetary policy interact, the appropriate role of liquidity and capital regulations, and the importance of taking a balanced approach to supervision and regulation, which supports both financial system resilience and the ability of financial firms to offer sound credit, liquidity, and payments services throughout the business cycle. Regulatory changes and the steps bankers themselves have taken to shore up their risk-management practices have led to a stronger and safer financial system.

But as much as we have learned and accomplished, there is still more to do. The financial system is dynamic: it is constantly evolving. Technological change is happening at a rapid pace. Machine learning, artificial intelligence, distributed ledgers, and other technological advances all hold the promise of making our financial and payments systems more efficient and effective for more people and of creating better analytical tools with which to monitor and manage risks. But these advances also pose challenges and have the potential to create new risks and imbalances that may be more difficult to monitor. With the advent of new technologies, some firms offering financial services do not fit neatly into the current

regulatory framework, and monitoring risks outside of the traditional banking sector presents some challenges. In a financial system that is rapidly adopting new technologies, our knowledge can rapidly become obsolete, as can the constructs we use to monitor and manage risks to financial stability. When the nature of the risks is changing, we need to ensure that our methods of assessing risks are nimble enough to adapt to the changing landscape.

In my limited time this morning, I will focus on one area of rapid change pertinent to financial stability: namely, the risks to cybersecurity and our ability to handle these risks. Of course, the views I will present today are my own and not necessarily those of the Federal Reserve System or my colleagues on the Federal Open Market Committee.

Cybersecurity and Financial Stability

As businesses have become more reliant on technology, efforts to disrupt a financial institution's operations; to steal, corrupt, or destroy data and intellectual property; or to divert funds have become more prevalent. As the Financial Stability Board points out, several recent events show the sizeable damaging effects such cyber incidents can have on the financial system. These include the attack on the Bangladesh Bank in 2016, which resulted in the theft of $81 million; the WannaCry ransomware attack in 2017, which infected more than 250,000 computer systems in 150 countries; and the Equifax hack in 2017, which compromised the personal information of over 146 million people.[1]

It is difficult to come up with firm numbers about the costs of malicious cyber activity – a fact that itself indicates we need to do more to monitor these risks. The U.S. Council of Economic Advisers has estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016, and other estimates suggest that those costs are rising rapidly, by 23 percent between 2016 and

[1] Financial Stability Board (2018).

2017 according to one study.[2] Firms are spending significant amounts on their cybersecurity, with one estimate at nearly $124 billion globally in 2019.[3] While all businesses face cyber risks, the stakes are particularly high in the financial services industry, given the critical role the financial system plays in the overall health of the U.S. and global economy.

One might be tempted to view cyber risk as a form of operational risk and treat it within the frameworks we have already established for assessing such risks. Instead, I think it pays to put cyber risks into a special category,[4] recognize they are becoming increasingly sophisticated, and realize that creative new solutions are needed to monitor and mitigate these risks. Cyber attacks have become more systematic, maliciously targeting financial firms and playing out over time for maximum effect. Detection can be difficult; an institution may believe it has backed up its good data, but those data may already have been compromised by malicious code that has infiltrated the institution's system. Data integrity will increasingly need to be a focus as firms develop plans for how they will recover from the inevitable attack. As financial institutions have adopted new technologies, sometimes through third-party suppliers, they are susceptible to risks that they may not have faced before. Those making the attacks are also adopting new technologies that more easily exploit gaps in financial firms' information technology, payment messaging and transaction authorization systems, and supply chains, which can widen the extent of the attack and make response or recovery more difficult. In such a landscape, weaknesses in financial firms' governance and communications structures – for example, not being clear about who has the decision rights to turn off a system, or what effect turning off one system will have on other systems – can exacerbate problems faced by a firm under attack.

[2] Council of Economic Advisers (2018) and Kashyap and Wetherilt (2019).

[3] See Kashyap and Wetherilt (2019).

[4] Kashyap and Wetherilt (2019) and Healey, et al. (2018) discuss how cybersecurity differs from other types of operational risks in the financial sector.

Instead of being idiosyncratic and affecting only a few firms, as many operational risks are, cyber threats are more likely to be correlated across institutions because of the complex interconnections and dependencies among financial firms. This means that cyber threats are more likely to have wider spread, and potentially systemic, negative impacts than a typical operational problem that might arise from a failed system or process. Trading platforms, settlement and payments systems, and central securities depositories are all critical infrastructures on which financial firms depend, and if these systems go down, there are few substitutes. In addition, the advent of new technologies and the move to cloud computing create additional concentrated risk, as only a handful of third-parties provide these services.

As much as individual firms are investing in cybersecurity – and it is a lot – as a nation and globally, we are likely underinvesting. This is because cybersecurity is a public good: the overall financial system conveys benefits to us all. Individual institutions certainly have incentives to invest in their own cybersecurity. As they have considered the tradeoff between the risk of loss to their firm from a cyber attack versus the cost of protection, financial services firms have been making major investments to monitor and protect their systems against attack. But the social benefit conveyed by a well-functioning and resilient financial system, one in which the public can continue to have a lot of confidence, requires a higher level of investment in cybersecurity than what individual firms would decide to do on their own. In addition, many individual firms rely on shared services. In considering how much to invest in their own cybersecurity, each firm should be entertaining the possibility that those shared services could come under significant stress in the event of a major attack on multiple firms at the same time [5] or that the shared service itself could be the entry point for a system-wide attack. These types of externalities may not be part of any one firm's investment decision. In addition, there could be free-rider problems: an

[5] See Kashyap and Wetherilt (2019).

individual firm may rely on others in the shared network to make investments to increase the security of the network, but if every firm thinks this way, there will be underinvestment in security.[6]

Cybersecurity and the Federal Reserve Bank of Cleveland

Given the changing environment, both financial services firms and their supervisors are making cybersecurity a high priority. In fact, because the stakes are so high, the banking industry is one of the most responsive industries in efforts to combat cybersecurity threats. Banks have strengthened their defenses and are detecting breaches in a more timely manner, shortening the time it takes to detect a problem once an attacker has entered a system.[7] Institutions are engaging in tabletop exercises, enhancing their incident response playbooks, and testing systems to strengthen their ability to recover from attacks. Firms are testing applications within sandboxes and using artificial intelligence to help detect cyber intruders. Realizing their common interests in effectively managing these risks, financial firms have been working on some joint efforts. Sheltered Harbor is an industry initiative that provides participant financial institutions a way to store data independent of the bank's own infrastructure. This can help make recovery quicker after an attack is detected. Sheltered Harbor reports that as of March 2019, its members accounted for 71 percent of U.S. deposit accounts and 55 percent of U.S. retail brokerage client assets.[8]

Cybersecurity is a high priority for the Federal Reserve. The Fed's approach builds on techniques that we have successfully applied to other forms of financial system oversight. We are developing clear and consistent standards for assessing financial institutions' preparedness and establishing corporate governance best practices with respect to cybersecurity. We are also acquiring and deploying Fed staff

---

[6] Sablik (2017) discusses the underinvestment problem. See also the Council of Economic Advisers (2018). The U.S. Department of the Treasury (2013) outlines the role government incentives can play in driving private-sector actions to strengthen defenses against cyber threats.

[7] See FireEye Mandiant Services (2019), p. 7. Across industries, the median detection time in North and South America has fallen from 99 days in 2016 to 71 days in 2018.

[8] See shelteredharbor.org for further information.

with the necessary technical skills to assess risk-management practices at financial firms, and we are encouraging and creating avenues for information sharing among financial institutions and regulators. The Fed has increased coordination with the other federal banking agencies in assessing cybersecurity at the nation's largest, most complex firms. We are aligning what we expect of banks in terms of identifying, protecting, detecting, responding to, and recovering from cyber attacks with the best-practice standards in the National Institute of Standards and Technology's (NIST) cybersecurity framework.[9] The banking agencies coordinate their annual reviews of the large, complex institutions, targeting key areas of supervisory interest, including cyber governance and risk management, incident response, and the ability to restore critical services. We have raised the expectations of cyber preparedness for all of the institutions we supervise, including regional and community banks.

The Cleveland Fed is playing an important role in the Federal Reserve's cybersecurity initiatives in several ways. Since 2015, the Cleveland Fed has been co-leading the Federal Reserve System's annual national horizontal review of cybersecurity for banks with assets between $100 billion and $500 billion. Fed examiners assess a bank's cybersecurity along a number of dimensions. Effective cybersecurity requires sound cyber-risk governance, including leadership's engagement in oversight of the firm's cybersecurity programs. An institution needs to have effective programs for identifying and managing risks and vulnerabilities, including those within its own technology infrastructure, those associated with vendors and third-party technology providers, and those posed by new products. Examiners assess a bank's incident response and recovery plans, as well as basic elements of good cyber hygiene, such as adequate technology inventories; safeguards for hardware, software, and customer and transaction data; and access and patch management.

[9] See Quarles (2018)

The Cleveland Fed is also playing a national role in the collection of threat information. The Federal Reserve System's Cybersecurity Analytics Support Team (CAST) was created in 2015 and is based at the Cleveland Fed.[10] This team tracks the latest cybersecurity developments across the U.S. financial sector in critical payment, clearing, and settlement systems, allowing it to gain a wide perspective on potential threats to the overall financial system and to better calibrate threat severity and impact. As its name implies, Cleveland's CAST group casts a wide net in its 24 hours a day, seven days a week, 365 days a year monitoring of cybersecurity risks in the financial system, working with the U.S. Department of the Treasury, other bank regulatory agencies, and the FBI. The Cleveland Fed staff is sharing its expertise on cybersecurity topics at industry and regulatory forums, and last month held its second conference on managing cyber risks, with financial industry risk and information security officers participating.

The Federal Reserve is a provider of both wholesale and retail payment services to the public and the U.S. government, and we recently launched a project called FedNow, to build a real-time gross settlement system to promote a safe and efficient faster payments system available to all. We need to maintain the public's trust and confidence in our ability to deliver those services, so we are highly engaged in work to enhance the resilience of our own systems, applications, and data against cybersecurity risks. The Cleveland Fed is one of the four Reserve Banks that provide payment services to the U.S. Treasury. Our eGov function focuses on revenue collections and eCommerce on behalf of the U.S. Treasury's Bureau of the Fiscal Service, maintaining and operating multiple systems for collecting funds for federal government agencies and providing solutions to take advantage of newer payments technologies. In addition to managing operational risks, our staff is constantly monitoring cybersecurity risks and potential fraudulent transactions on these critical payments services.

[10] More information on the Cleveland Fed's work on cybersecurity is available on our website at https://www.clevelandfed.org/newsroom-and-events/multimedia-storytelling/cybersecurity.aspx.

Four Recommendations to Enhance Cybersecurity

While the financial services industry and the supervisory agencies have made significant progress, the cybersecurity landscape is constantly evolving amid rapid technological change. So let me offer four recommendations to enhance the cyber resilience of the global financial system.

First, financial system supervisory agencies need to become more agile to ensure that our supervisory frameworks are up to the task of monitoring cybersecurity. The Federal Reserve continues to work with the other federal banking agencies to harmonize our cybersecurity examination requirements, but progress has been slow. In October 2016, the three federal banking regulatory agencies published an advance notice of proposed rulemaking inviting comment on a set of potential enhanced cybersecurity risk-management and resilience standards. This draft guidance is still in process. Given the changes in technology, including the move to cloud technology, the supervisory program applied to the most critical third-party service providers needs to be updated. We need to become agile in our approach to supervision; otherwise, changes in technology will overtake our ability to monitor and manage risks.

Second, given the systemic nature of cyber risks and the potential for widespread disruption, further collaboration between the regulators, government, financial institutions, and other private-sector firms will be a crucial ingredient for improving our cybersecurity. One form of this collaboration is tabletop exercises, which can improve the readiness of the industry and the government to respond to a cyber incident. The Fed participates in the Hamilton Series of tabletop exercises, in collaboration with the U.S. Department of the Treasury and the Financial Services Information Sharing and Analysis Center (FS–ISAC), an important banking industry forum that promotes collaboration on critical security threats. These exercises are intended to improve public- and private-sector management of cyber risks. Participants have told us that they value these exercises because they promote consistent approaches and best practices in event response and recovery and they foster relationships with key regulatory officials.

Because cyber threats are not restricted by national borders and because the financial system is interconnected, cross-border collaboration must also advance. In November 2015, the U.S. and U.K. governments conducted a joint exercise with leading global financial firms to determine how the two governments would perform in the event of a large cyber attack on the financial systems in both countries.[11] The Fed participated in the exercise, which evaluated incident-response handling and recovery, coordination, public communication, and information handling. These types of exercises should be expanded and carried out on a more frequent and regular basis. This will help those who have not been exposed to such situations learn how to handle them and allow the lessons to become second nature to all bank and supervisory staff.

Third, further development and use of stress testing to assess the financial system's resilience to cyber risks are needed. Just as horizontal stress testing has proven to be a useful tool in assessing the overall resilience of the financial system to credit and liquidity risks, stress testing could be used to assess how prepared individual firms and the overall system are to respond to and recover from a systemic cyber event such as the shutdown of a major clearing or settlement bank. Such a test could help evaluate the financial system's plans for data and core systems recovery and its reliance on third parties to implement that plan. As part of the recovery plan, data integrity needs to be a focus: how can the institution ensure that the data it backed up have not already been altered?

The G7 has provided a guide to authorities for assessing resiliency through the use of simulations, such as threat-led penetration tests. To test the resiliency of an institution's systems and its ability to recover from an attack, these tests are carried out without advance knowledge using the techniques and tactics of actual malicious attackers.[12] The Bank of England is applying stress-testing techniques to evaluate whether financial firms are able to resume services within the tolerance set by the Bank of England in the

[11] See U.S. Department of the Treasury (2015).

[12] See G7 Cyber Expert Group (2018).

face of a system-wide attack or data corruption that affects multiple firms and their service providers.[13] Adapting and adopting some of these practices in the U.S. would be worthwhile.

Fourth, information gathering, sharing, and analysis need to be promoted as critical ingredients for improving our cybersecurity. The Financial Stability Board recently published a cyber lexicon.[14] A common language is crucial to ensure consistent data collection and reliable measurement. Another crucial ingredient for effective monitoring is firms' willingness to share information on cyber incidents. Without such sharing, it is much harder to develop metrics to evaluate cyber resilience, to assess whether threat levels are rising or beginning to propagate through the financial system, and to determine whether the practices firms have in place actually are working to mitigate the risks. So the Fed has been working with FS-ISAC to promote information sharing.

But collecting and sharing the data are not enough. With the constant evolution of the threats, advanced techniques for analyzing those data need to be developed so that evolving trends can be identified. Here, technological advances like machine learning and artificial intelligence can be helpful, if applied correctly. But if not applied correctly, they can result in false positives, diverting attention from actual risks and vulnerabilities. Given that the necessary skill sets are difficult to acquire, especially by regulatory agencies without deep pockets, the agencies should be willing to develop appropriate collaborations with universities and other entities with an aptitude and interest in using such techniques for the good of the public.

In summary, my four recommendations are: an agile supervisory framework for cybersecurity; global industry and agency collaboration; cybersecurity stress testing; and more robust data gathering, sharing, and analytics about cyber incidents. I see these areas as those in which the most urgent actions are needed

[13] See Kashyap and Wetherilt (2019).

[14] See Financial Stability Board (2018).

to help promote the resilience of our financial system. Given the nature of the financial services industry, with interconnections and dependencies on third-party providers, and advances in technology, this list can be expected to evolve. I hope it evolves because we have made significant progress in these four areas and not because the list has expanded to include new vulnerabilities that could have been avoided had we made better progress.

References

Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018.
(https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf)

Financial Stability Board, "Cyber Lexicon," November 12, 2018.
(https://www.fsb.org/wp-content/uploads/P121118-1.pdf)

FireEye Mandiant Services, "Special Report: M-Trends 2019," 2019.
(https://content.fireeye.com/m-trends)

G7 Cyber Expert Group, "G7 Fundamental Elements for Threat-Led Penetration Testing," October 15, 2018.
(https://www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf)

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache, "The Future of Financial Stability and Cyber Risk," The Brookings Institution Cybersecurity Project, October 2018.
(https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/)

Kashyap, Anil K., and Anne Wetherilt, "Some Principles for Regulating Cyber Risk," *American Economic Association Papers and Proceedings* 109, May 2019, pp. 482-487.
(https://pubs.aeaweb.org/doi/pdfplus/10.1257/pandp.20191058)

Quarles, Randal K., "Brief Thoughts on the Financial Regulatory System and Cybersecurity," at the Financial Services Roundtable 2018 Spring Conference, Washington, D.C, February 26, 2018.
(https://www.federalreserve.gov/newsevents/speech/quarles20180226b.htm)

Sablik, Tim, "Cyberattacks and the Digital Dilemma," Econ Focus, Federal Reserve Bank of Richmond, Third Quarter 2017.
(https://www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2017/q3/cover_story.pdf)

U.S. Department of the Treasury, "Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636," 2013.
(https://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf)

U.S. Department of the Treasury, "Joint Statement from the U.S. Department of the Treasury and Her Majesty's Treasury," November 12, 2015.
(https://www.treasury.gov/press-center/press-releases/pages/jl0262.aspx)