# Cybersecurity and the Federal Reserve


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

**Fourth Annual Managing Cyber Risk from the C-Suite Conference**
**Sponsored by the Federal Reserve System's Large and Foreign Banking Organizations Management Group**

**Federal Reserve Bank of Cleveland**
**Cleveland, OH**
**(via videoconference)**

**October 5, 2021**

**Introduction**

It is a pleasure to welcome you to this year's conference on Managing Cyber Risk from the C-Suite. This is the fourth annual conference in this series, and each year the discussions have both broadened and deepened our understanding of the cyber risks faced by the financial system. It is hard to get through a week without hearing about a new cybersecurity event that has affected an organization and its customers. These events impose costs and affect operations at institutions of all sizes. Efforts to disrupt an institution's operations; to steal, corrupt, or destroy data and intellectual property; or to divert funds have become more prevalent. According to Boston Consulting Group, financial services firms are 300 times as likely as other types of companies to be targeted by a cyber attack.[1] Just as the financial system is constantly evolving, so, too, are the cybersecurity risks that institutions need to assess and manage. Given the vital role that financial services firms play in supporting a strong global economy – a role clearly demonstrated throughout the pandemic – it behooves us all to continually expand our knowledge of the risks we face and the best way to combat them.

**Cybersecurity and Financial Stability**

Given the Federal Reserve System's role in fostering a strong economy and a stable financial system, cybersecurity is a high priority for us. To put it succinctly, there is no financial stability without cybersecurity. Indeed, at a recent European Central Bank Forum, Fed Chair Jay Powell said that a successful cyber attack on a large financial institution or financial market utility is one of the top risks to financial stability.[2] And surveys indicate that this view is widely shared by the industry and other

[1] See Anna Zakrzewski, Tjun Tang, Galina Appell, Andrew Hardie, Nicole Hildebrandt, Michael Kahlich, Martin Mende, Federico Muxí, and André Xavier, "Global Wealth 2019: Reigniting Radical Growth," Boston Consulting Group, May 2019, p. 22. (https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf)

[2] European Central Bank Forum on Central Banking 2021, policy panel with Andrew Bailey, Haruhiko Kuroda, Christine Lagarde, and Jerome H. Powell, moderated by Alessandra Galloni of Reuters, September 29, 2021.

financial regulators across the globe.[3] While much progress has been made in addressing more typical banking risks, including credit, liquidity, and operational risks, risks to cybersecurity are expanding, very dynamic, and becoming increasingly sophisticated. Cyber attacks have become more systematic, maliciously targeting financial firms and playing out over time for maximum effect.

Cyber threats pose some unique hazards to financial stability. Because of the complex interconnections and dependencies among financial firms, cyber threats are more likely to be correlated across institutions and to have wider-spread negative effects than a typical operational problem. An attack that compromises an institution's system or data can impair its ability to service creditors not directly affected by the attack. In addition, an attack on a trading platform, a settlement and payments system, or a central securities depository could have a major impact on the financial system as a whole because these are critical infrastructures on which financial firms depend and for which there are few substitutes. The advent of new technologies like cloud computing creates another concentrated risk, as there are only a handful of third-party providers of these services. Cyber risk can also be amplified by coordination failure. Decision-making tends to be decentralized across financial institutions and across global financial regulatory agencies; so without prior engagement, guidance, and proper communication channels, a small attack can be propagated across the system.

A recent Federal Reserve study analyzed the potential impact of a hypothetical cyber attack on the five largest participants in the U.S. wholesale, large-value payments network, called Fedwire. Because these large players account for close to 40 percent of total payments on the system, an attack on these institutions would have spillover effects on others, with an average spillover impact on about 38 percent of banking system assets, excluding the attacked institutions. Because of the nature of Fedwire, the institutions under attack would be able to receive funds but not send them out, and in the simulation, the

[3] See Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," Federal Reserve Bank of New York *Staff Reports*, No. 909, January 2020, revised May 2021. (https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf)

average liquidity shortfall in the financial system would grow from $122 billion on the first day of the attack to $1 trillion by the fifth day.

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, and banks 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, likely requires a higher level of investment in cybersecurity than what individual firms would decide to do on their own, as they consider the tradeoff between the risk of loss to their firm from a cyber attack versus the cost of that investment. In addition, to the extent that individual firms are relying on shared services, in considering how much to invest in their own cybersecurity, they should be entertaining the possibility that those shared services could be heavily taxed in the event other firms are attacked at the same time they are [4] 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. Moreover, an individual firm may rely on others in the shared network to make investments that make the network more secure, but if every firm thinks this way, there will be underinvestment in security.[5]

**Cybersecurity and the Federal Reserve System**

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

[5] See Tim Sablik, "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); and 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)

The public good aspect of cybersecurity and the Federal Reserve's role in ensuring the resiliency of the financial system mean that the Fed has a role to play in helping the financial services industry improve its ability to prevent, detect, and recover from cyber attacks. We are making sure we are doing the same with our own payments systems. Because attacks continue to grow in sophistication, even the best cyber controls will not be able to stop all determined attackers; so ensuring operational resiliency is critical. An institution's being prepared for and having the ability to withstand and effectively recover from an attack are becoming increasingly important. From a systemic resiliency perspective, banks' timely notification to their supervisory authorities when an incident occurs can be a big help. As the Fed improves the efficiency and speed of services like Fedwire, and as we develop the FedNow[SM] instant payments system, timely reporting is becoming even more important, since it will allow us to coordinate a systemic response that minimizes service disruptions in the event multiple firms are simultaneously attacked.

In order to promote financial system resiliency, the Fed has taken steps to ensure that our supervision of banks' cyber security posture is effective. We have been developing clear and consistent standards for assessing financial institutions' preparedness; establishing corporate governance best practices with respect to cybersecurity; hiring staff with the necessary technical skills to assess risk-management practices; and 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 coordinating our annual reviews of these institutions, targeting key areas of supervisory interest, including cyber risk-management practices and the resiliency and recovery of critical services. This coordination has the added benefit of reducing the regulatory burden for institutions subject to oversight from multiple regulators while making that oversight more effective. We have also raised our expectations of cyber resilience preparedness for all of the institutions we supervise, including regional and community banks.

The Fed is also focused on enhancing our own cybersecurity. The Fed is a provider of both wholesale and retail financial services to the public and the U.S. government. We need to maintain the public's trust and confidence in our ability to deliver those services. The Fed has remained secure from ever-growing cybersecurity threats. But we do not take that for granted. We are continuously working to enhance the cyber security and resiliency of our own systems, applications, and data, to ensure that we can detect and prevent an attack on our systems, and if one were to occur, making sure we can minimize the time it takes to contain it and limit the business impact on our customers. We regularly obtain cyber intelligence on how actors may attempt to attack critical Federal Reserve payments systems, we regularly test our controls to determine their capabilities in preventing these attacks from being successful, and we are continuously improving and testing our preparedness against a potential ransomware attack, which is a top threat for organizations, including the Fed. The Cleveland Fed provides critical payments services to the U.S. Treasury, including operating several systems to collect funds for federal government agencies. Our staff is constantly monitoring cybersecurity threats and potential fraudulent transactions on our systems.

**Cybersecurity and the Federal Reserve Bank of Cleveland**

The Cleveland Fed is taking a leading role in the Federal Reserve System's cybersecurity efforts more broadly. The System's Cybersecurity Analytics Support Team, known as CAST, is based at the Cleveland Fed. This team monitors and analyzes threats faced by institutions supervised by the Federal Reserve. The Cleveland Fed recently collaborated with the Ohio Department of Commerce's Division of Financial Institutions' Technology Advisory Group to develop and perform a tabletop ransomware cyber attack exercise to help banks improve their preparedness. The exercise used the latest intelligence from CAST on how ransomware can rapidly compromise an entire network of computers and how attackers attempt to extort payments from firms in exchange for decryption keys and promises to not release stolen customer information.

We regularly share information and cyber security insights with the management teams of our District's large banks. This information sharing has been especially important during the pandemic. The Cleveland Fed was able to identify and alert firms to new cyber risks that were rapidly arising as banks were transitioning to remote work. Later today, Chad Siegrist, who heads CAST, will share the latest information on ransomware, phishing attacks, account hijacking, and other methods of cyber attacks targeted at banking organizations.

Advancing cybersecurity supervision is one of the strategic goals of the Cleveland Fed's supervision function. The Cleveland Fed participates in 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. The bank 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. The bank is assessed on its processes for incident response and its plans for timely recovery and restoration of critical functions, as well as on the basics, such as adequate technology inventories, data security, access management, and timely software patching. Our next speaker, Jennifer Burns, who is the deputy director of supervision and regulation for the Federal Reserve System, will share more information about the Fed's cyber examination program.

**Conclusion**

I hope my brief remarks have made it clear why the Federal Reserve is so focused on cyber resiliency and what we at the Cleveland Fed are doing to advance both the industry's and the Fed's own resiliency against cyber incidents. The dynamic nature of the cyber landscape, with rapid technological change and ever-evolving risks that are becoming more sophisticated and complex, can make it seem like we are always running to catch up. This can be discouraging. But if one looks back over the previous years of

this conference, it is clear that much progress has been made in better understanding cyber threats and how, by working together, we can best handle those threats. My expectation is that perseverance and collaboration will continue to yield benefits in making our financial system ever more resilient. And this resiliency is critical, given the importance of the financial system to our economic health.