Michael S Barr: Measuring cyber risk in the financial services sector

Opening remarks by Mr Michael S Barr, Vice Chair for Supervision of the Board of Governors of the Federal Reserve System, at the conference on Measuring Cyber Risk in the Financial Services Sector, Boston, Massachusetts, 17 January 2024.

* * *

Thank you for the opportunity to welcome you to day two of the second annual Conference on Measuring Cyber Risk in the Financial Services Sector.[1] I'd like to thank the staff who organized this gathering from the Massachusetts Institute of Technology, the Federal Reserve Bank of Richmond, and the Federal Reserve Board.

Cyber threats are constantly evolving, and we can expect them to become increasingly disruptive as technology advances and our financial system becomes more interconnected. In the past few months, ransomware attacks have disrupted the ability of some financial institutions to offer a variety of banking and market services, including Treasury clearance and settlement and access to online banking and ATM operations. These incidents were resolved without significant disruption to the broader market, but they are stark reminders of the potential for cyber incidents to generate broader, even systemic risks, and the importance of addressing these risks.

Cybersecurity preparedness has become increasingly important for banks. Banks must take action to uncover vulnerabilities in their systems and remedy those vulnerabilities before attacks occur. But focusing on cyber defense is not sufficient. It is important that banks also focus on resilience to successful cyber-attacks, including by developing and regularly testing business continuity plans.

The Federal Reserve and other banking agencies work to make sure that banks and service providers are appropriately focused on cybersecurity and operational resilience. Supervisors will continue to reinforce the need for appropriate risk management.

Reliance by banks on third-party service providers has grown considerably in recent years, and with that reliance comes the potential for greater cyber risk.[2] It is ultimately the responsibility of banks to manage their third-party risk, and we have historically seen gaps in this regard. Last year, together with the other bank regulatory agencies, the Federal Reserve adopted guidance on effective management of third-party risk, based on the size and complexity of the bank and nature of the third-party relationship. The guidance provides some specific examples throughout the lifecycle of a third-party relationship, which should be helpful for banks as they strengthen their management of these risks.

Forums like today's conference are critical to improve how we think about and measure the presence of cyber risk in financial markets. The ability to better measure cyber risk will allow banks and supervisors to improve their understanding of the direct and indirect costs of a cyber disruption. An incident poses direct costs on an affected bank and its customers, as well as indirect costs to other market participants who are connected to the affected bank. For instance, researchers at the New York Federal Reserve Bank recently modeled how a cyber incident could be transmitted through the

U.S. financial system under a variety of circumstances.[3] The authors estimate how the impairment of a single large bank, a group of smaller banks, or a common service provider could be transmitted through the payments system and result in significant spillovers to other banks. Spillovers to the broader financial system are estimated to be especially large when attacks are timed to maximize damage, further highlighting challenges that arise with protecting against cyber risk. In addition, the researchers estimate that the potential impact of a cyberattack is systematically greater during stressed financial conditions. This indicates that we need a deeper understanding of how cyber risk interacts with traditional challenges to financial stability.[4] Many of the participants in today's conference are working on research that will advance our knowledge of cyber risk and financial stability, and I am looking forward to continuing to follow work in this area.

Despite progress in recent years, techniques to quantify cyber risk are still at a nascent stage, in part because of a lack of good data. Better data on cyber threats and vulnerabilities will enable us to identify and assess threats to banks and the financial system. In addition, improved data on interconnectedness between financial institutions and service providers will help identify and measure the impact of an incident on the broader financial system. The ability to quickly identify patterns, connections, and vulnerabilities will enable quick response, and may mean the difference between a controlled event and one that has a serious impact. We are supporting efforts to further study this subject through public-private coordination groups. In addition, cyber incident reporting will provide better data on the frequency, severity, and locality of cyber incidents that will enhance our collective ability to respond to these events.

I am heartened to see that many of the attendees and speakers at this conference come not just from the United States, but also from around the globe. Today's globalized financial system and the global nature of cyber threats demand international coordination from both participants and regulators. In closing, I look forward to hearing more about what you all accomplish during the remainder of the conference, in furtherance of a more resilient financial system.

Thank you.

---

[1] The views expressed here are my own and are not necessarily those of my colleagues on the Federal Reserve Board.

[2] See, e.g., Kotidis, Antonis, and Stacey L. Schreft (2022). "Cyberattacks and Financial Stability: Evidence from a Natural Experiment," Finance and Economics Discussion Series 2022-025. Washington: Board of Governors of the Federal Reserve System.

[3] Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, "Cyber risk and the U. S. financial system: A pre-mortem analysis," *Journal of Financial Economics*, Volume 145, Issue 3 (September 2022): 802–826, https://www.sciencedirect.com/science/article/pii/S0304405X21004578?via%3Dihub.

[4] Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee, "When It Rains, It Pours: Cyber Risk and Financial Conditions," (Federal Reserve Bank of New York, last modified August 2023).