For release on delivery
2:10 p.m. EDT (1:10 p.m. CDT)
June 25, 2024

Opening Remarks

by

Michelle H. Bowman

Member

Board of Governors of the Federal Reserve System

via prerecorded video

at

The Midwest Cyber Workshop
The Federal Reserve Banks of St. Louis, Chicago, and Kansas City

St. Louis, Missouri

June 25, 2024

Good afternoon and welcome to the 2nd annual Midwest Cyber Workshop hosted by the Federal Reserve Banks of Chicago, Kansas City, and St. Louis.[1] This workshop was launched last year to further the conversation on cyber risks between community bankers, regulators, law enforcement, and industry stakeholders. It is an honor to be a part of this workshop again and to kickoff this year's event.

Cybersecurity continues to be a key risk area for the banking industry and for regulators. Cyber-related events, including ransomware attacks and business email compromises, are extremely costly and time-consuming experiences. For community banks, maintaining the necessary resources and technology to support a successful cybersecurity program can feel especially challenging and financially burdensome. The evolving nature of cyberthreats requires banks to continually review and enhance processes and procedures to protect, detect, and respond to an incident, even if the operating environment has not significantly changed. Ten years ago, immutable backups and multifactor authentication on privileged access accounts were not common controls deployed by community banks. Today, they are considered to be standard elements of a cyber risk management strategy.

Financial industry vendors and service providers add an additional layer of cyber-related vulnerability. Attacks on these third parties have enabled bad actors to create operational incidents and breaches of customer information at financial institutions. Effectively managing and monitoring third-party relationships is an essential component of a bank's broader risk management function. Given the increased adoption of cloud-based solutions, outsourcing of critical functions, and exploration of the use of artificial

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

intelligence (AI), banks must have robust strategies for cyber resilience. Generative AI has the potential to transform operations and the customer experience. But it is also vulnerable to cyberthreats and will require an ongoing analysis of risk-identification and -management.

Last year, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency jointly issued new guidance titled "Interagency Guidance on Third-Party Relationships: Risk Management," which was recently supplemented by a community bank guide meant to assist these banks in tailoring their third-party risk management programs. Later this afternoon, you will hear more on this from our panel of IT examiners on these resources, recent observations from the field, and risks associated with AI.

Ransomware attacks continue to target individuals, businesses, and governments across the country and often result in significant financial and operational harm. Combating ransomware requires that an organization make investments in people, processes, and technology. Often, these attacks are successful because well-intentioned staff have their guard down, or they are not effectively trained to identify and respond to a potential incident.

Employees can be your greatest strength, but also your weakest link when it comes to protecting digital assets. That's why it is critical that cyberprograms are built upon a solid foundation that includes training staff to quickly respond to suspicious activity. This reinforces the importance of a skeptical approach in helping to safeguard information. Today and tomorrow, Federal Reserve staff, law enforcement, and industry stakeholders will share their perspectives on ransomware incidents, including restoration

of key payments-related functions, cyberinsurance, payments-related risks, and financial considerations during an incident.

Finally, a cybersecurity program would not be complete without a comprehensive testing and exercise plan. By incorporating regular testing, a bank can identify strengths and weaknesses in their current strategies. They can then leverage this information to enhance resiliency, resulting in a higher level of preparedness when an incident occurs. Tabletop exercises like the one facilitated tomorrow with IBM are an excellent way to test a cyberdefense strategy against multiple scenarios, including those involving a third party and payment systems.

In closing, outreach events like this workshop, the February 2024 Ask the Fed® session with the Cybersecurity and Infrastructure Security Agency, and our recent virtual "office hours" on the 2023 third-party risk management guidance enable us to connect and share resources. These opportunities help us to better support industry management of cybersecurity and other operational risks.

I would like to thank the Federal Reserve Banks of Chicago, Kansas City, and St. Louis for organizing this event, and I hope you enjoy the workshop.