BOARD OF GOVERNORS *of the* FEDERAL RESERVE SYSTEM

Cybersecurity in the Financial Services Sector

September 27, 2017

Nida Davis
Associate Director,
Supervision and Regulation Policy
Federal Reserve Board of Governors

Disclaimer

- The views expressed in this presentation are individual views, intended for informational purposes, and are not formal opinions of, nor binding on, the Federal Reserve Board.

Technology in the financial sector

- Mobile banking and other technologies are increasingly becoming the norm for how consumers access their money and conduct transactions.
- Reliance on third-party services has increased and changed financial services business models.
- While business and consumer demands are driving increased innovation, risks to individual firms and the overall sector must be addressed.
- Increased reliance on technology increases the interconnectedness and interdependencies between firms, which increases systemic risk to the sector.

Business technology risk

- Technology is a business enabler, however it represents increasing risks to firms.
- Business technology risk touches all aspects of a firm's operations and includes people, processes, systems, risk management, resilience, etc..
- Information technology is no longer a back office function; cyber risk has elevated it from the server room to the board room.

Risks due to the adoption of technology in banking

- Technology may increase a firm's customer base and bottom line but also increases risks associated with theft and fraud.

- Fraud conducted through cyber means is on the rise with ATM cash-out schemes, identity theft, and fraudulent wire transfers being the most highly visible techniques.

- Poor cyber hygiene is a large contributing factor in successful cyber attacks.

- Cyber attacks may result in financial, legal and reputational risk issues.

Current state of cyber threats

- The rise in frequency and sophistication of cyber threats can be attributed to various types of threat actors.
- Retail financial institutions and their customers are the primary targets in the financial sector for financially motivated cybercriminals.
- Existing vulnerabilities continue to be exploited.
- New platforms create new cyber attack opportunities.

What can firms do to better manage cyber risk?

- Basic cyber hygiene is fundamental in protecting an organizations' assets and detecting a cyber incident.
- Information sharing with other firms across the sector or with related sectors is a crucial component to effective cyber defense.
- Having sound risk management practices set the foundation for firms to be better prepared when impacted by a cyber attack.
- Increased emphasis on cyber resiliency as a key component of a firm's cybersecurity preparedness.

What can boards of directors and management do?

- Maintain investments in IT infrastructure to ensure that systems are fully supported by vendors and that they incorporate effective security and resiliency solutions.

- Ensure there is a complete inventory of applications and connections to the Internet and incorporate these dependencies into operational resiliency plans that are tested as threats change.

- Obtain and act on timely information regarding vulnerabilities and mitigations.

- For outsourced services, enhance oversight of third parties including their cybersecurity risk management programs and tests of contingency plans and operations.

What is the role of Federal Reserve supervision?

- Guidance on risk management and operational resilience is available in the FFIEC IT Examination Handbooks, which are updated periodically to incorporate industry best practices and standards.
- Supervisory examinations are risk-based and account for a firm's size and complexity.
- Tools and resources are available for firms to use to assess the effectiveness of cyber risk management practices.
- Collaboration and coordination with other financial regulators and other government agencies.

Questions

?