Oversight of Cyber Resilience in the Financial Regulatory System

Seminar for Senior Bank Supervisors from Emerging Economies

October 25, 2019

Art Lindo, Deputy Director for Policy, Federal Reserve Board

What do we mean by Cyber resilience and how does it differ from Cyber security?

- Cyber Resilience - The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.
- Cyber security - Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
    - Source: FSB Cyber Lexicon

What is the current perspective on Cyber resiliency and, more broadly, operational resiliency?

- Banks and other financial institutions are operating in an environment that is experiencing an extensive technology-led business transformation.
- Fundamental shifts in consumer expectations are driving unpresented demand for highly integrated, mobile, personal, and digital customer experience.
- The traditional regulatory approaches will not be adequate for meeting the challenges of this new environment.
  - This is requiring regulatory approach that is significantly different from those we use for capital, liquidity and the other major risk stripes.
- The perspective has shifted from a focus on what to do “IF” an operational disruption occurs to a “When” a disruption occurs.

What is the outlook for cyber/operational resiliency?

Resiliency capabilities must continue to improve in step with the growing threat landscape

- Adversaries only need to be successful once in order to disrupt systems, cause havic and profit illegally.
- Banks, in contrast, need to be on guard against threats all the time and need a viable recovery plan for incidents when they occur.

What are the components of an effective oversight program for cyber/operational resiliency in the financial regulatory system?

- Common assessment frameworks
- Robust risk Analysis, threat assessment and information sharing
- Complimentary examination approaches and testing expectations at the bank level and throughout the financial sector
- Expanded workforce training, efficient resource allocation and smarter coordination
- Real-time monitoring of the functions that are critical to the bank's operations and the operations of the financial system
- Effective incident management including a focus on lessons learned from previous incidents

What are the high level objectives for cyber/operational resilience in the financial regulatory system? ?

- Identify essential and systemically important “critical” functions at the firm and sector level to account for the materiality and potential impact that the failure to provide a certain function could have on the firm, the financial system and the broader economy.
- Promote a common understanding of such functions and shared services as key components of the overall resilience of the firm, the financial system and the broader economy.
- Enable the assessment and measurement of operational resilience at the firm and sector level in real time.
  - Develop a methodology for the assessment of operational resilience of critical functions and core business lines that maps interdependencies, identifies potentially systemic risks and cross-sector implications of disruptions.
- Ensure the programs are implemented in a consistent manner across jurisdictions and are yielding measurable results.

What is being done from a policy and regulatory perspective to promote a common understanding of cyber/operational resiliency?

- We have changed our focus from developing operational resiliency expectations that are primarily regulatory driven to developing expectations that are harmonized to leading industry standards and best practices and reflect significantly more input from firms before we establish specific resiliency tolerances.
  - This has slowed down the regulatory process but the objective is to incentivize firms to adapt their behaviors and make investments that achieve our safety and soundness and financial stability objectives.

Who are the some of the oversight groups for cyber/operational resiliency program of the financial regulatory system (US perspective)?

U.S. Domestic

- Federal Financial Institutions Examination Council
- Cybersecurity Forum for Independent and Executive Branch Regulators
- Communications Security, Reliability and Interoperability Council
- Financial and Banking Information Infrastructure Committee
- U.S. Department Homeland Security

International Groups

- Group of 7 Cyber Expert Group International
- IT Supervision Group
- Committee on Payments and Market Infrastructure - International Organization of Securities Commissions
- Senior Supervisors Group Cybersecurity and Operational Resilience
- Basel Committee on Banking Supervision

Public/Private Partnerships

- Financial Services Sector Coordinating Council
- Industry Trade Associations
- Secure Payments Task Force
- Financial Services - Information Sharing Analysis Center
- Federal Reserve Bank of New York Payments Risk Committee

What are the Basel Committee's cyber/operational resiliency related efforts for the financial regulatory system ?

- Basel Committee efforts on operational resilience, including Cyber, are focused on:
  - Developing measures of resilience to assess a banking organization's ability to adapt to changing conditions, withstand disruptions, and ensure rapid recovery
  - Assessing availability of systems response and recovery for critical functions across the sector from end to end under common industry-wide standards
  - Advancing financial stability by promoting resiliency within the financial sector critical infrastructure
- Prospective deliverables
  - Operational resilience definition and principles for managing operational resilience
  - Operational resilience related metrics to assess firms' availability, response and recovery and develop indicators and/or benchmarks

Questions