OFFICE OF FINANCIAL RESEARCH

Financial Research Advisory Committee Meeting
July 20, 2017

Discussion Topic: Cyber and Financial Stability Initiative

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 mandates Office of Financial Research (OFR) to study current and emerging financial stability risks and identify best practices in risk management for financial sector firms. Cybersecurity and operational incidents are a growing source of risk that no longer threatens only individual institutions. Today, it threatens overall financial stability as well, because financial transactions occur through complex, interconnected networks. Disruptions to operations at one institution could propagate throughout the network and result in a systemic crisis.

The OFR is uniquely positioned to study the financial stability threat from cyber and operational risks. We have the authority to look across the financial system and collect essential financial data from federal financial regulators and market participants. The OFR studies the structure of the different financial sectors by combining data from regulatory and commercial sources, which allows for analysis of potential damages from endogenous or exogenous shocks. This work also can help in developing policies for enhancing the stability and resilience of the financial system.

The OFR has developed a two-pronged research agenda in this area:

First: We focus on operational and cybersecurity risks. We look at event studies, current experience, and shared intelligence to understand what events are occurring and how they might threaten the financial system. We evaluate the financial system's resilience, the contribution of policy, and gaps in policy that could enhance resilience. We draw lessons from tabletop exercises and contribute to improving them. And, we forge relationships with others working on these issues.

Second: The other side of our research agenda is more technical and focuses on applying network analysis to identify operational and cybersecurity risks. As part of this investigation, the OFR is building maps that highlight interconnections within and across the financial sector. We are using these maps to help identify the key vulnerabilities present in and among different markets.

This part of our research agenda has four components:

1. **Source:** Detailed data on the financial system is vital for accurate analysis of risks and vulnerabilities. The OFR is using available data and acquiring more data to create detailed maps of the major financial markets. Our priority is complete data at the transactions level that yields dynamic current information. Granular transaction-level data is important for our analysis. The more transactions between two entities, the greater the chance of contagion when a cyber or operational incident occurs and the larger the market impact of any disruption. Time-series data is also important in understanding how financial market structures change over time and to analyze the effects of regulations. As the network changes, different threats and vulnerabilities may arise, so ongoing monitoring is critical.

2. **Significance:** We use financial data to compile information about the size of the financial entities at each node (participant or market or financial market utility) in the maps, the volume of trade going through each node, and other relevant data to study which nodes matter most for the stability of a market. The failure of one large node from an operational or cyber incident might matter less for stability than the failure of one small node depending on how those nodes are connected to the rest of the financial system. Analysis of the significance of individual nodes will shed light on these issues.

3. **Stability:** Our data will allow for research into the stability and robustness of financial markets and the overall financial system. Network statistics such as link density, average degree, and clustering will show us how interconnected each market is. More interconnected markets may lead to greater contagion in the event of an attack. Theoretical network defense models can be used to test for vulnerabilities in financial markets. Analysis of these models will help determine the most resilient network structures and security measures across different markets.

4. **Shocks:** The OFR will study the resilience of financial markets to random and targeted incidents. Random attacks can affect any node and may represent natural disasters or accidents. Targeted attacks instead focus on the most vulnerable parts of the network and may represent malicious actors with detailed knowledge of the system. Different defense strategies are necessary against the two types of attacks. We can determine which markets are better defended against one type of attack versus the other by analyzing the network data we obtain. Our analysis will highlight key vulnerabilities in specific markets.

Questions for Discussion

1. Which financial markets are the most important to analyze immediately for urgent operational or cyber risks?

2. What research approaches and models are important for investigating operational and cybersecurity risks?

3. What statistics and metrics are the most important for monitoring and analyzing operational and cybersecurity risks?