Measuring Cyber Risk in the Financial Services Sector: Conference Summary (Executive Summary)

Sponsored by
The Board of Governors of the Federal Reserve System
The Federal Reserve Bank of Richmond
The Massachusetts Institute of Technology – Internet Policy Research Initiative

14 Nov 2022
On September 7-8, 2022, The Federal Reserve Board of Governors, the Federal Reserve Bank of Richmond, and the Massachusetts Institute of Technology’s Internet Policy Research Initiative hosted over 300 experts from industry, government, and academia to discuss the status of efforts to **measure** and **track cyber risk** across the financial system. The group highlighted the need for better data, identified data and model needs, and issued a call for broad collaboration on metrics and models.

**Collaboration for better measurement**

The financial sector needs better cyber risk metrics to support security decision making, target risk thresholds, and ensure the efficient use of risk capital. **Tom Barkin**, the President of the Federal Reserve Bank of Richmond, called for the industry, governments, and academia to work together to develop taxonomies and metrics to bring cyber risk closer to the models we already have in the financial service sector for managing operational and credit risk.

**MIT Professor Andrew Lo** stated the challenge clearly, “you cannot manage what you cannot measure”. We simply do not have the data necessary to measure and manage risk because it has been too sensitive to share. He said the stakeholders should work together on some key metrics, however crude they may be, as a first step toward developing industry indicators and models that could eventually support securities that could be traded for risk mitigation.

**Identified data and model needs**

This lack of data is visible in the cyber insurance market. Cyber insurance coverage is estimated to be roughly 1% of total estimated losses each year – a sharp contrast to natural catastrophe insurance where covered losses account for nearly 43% of total losses. The fundamental reason for this gap is a lack of data and the nature of cyber risk is twofold. First, data is scarce because the data is extremely sensitive, and firms are reluctant to disclose them. Second, cyber risk modeling is characterized by heavy tail distributions, non-linear dependencies, modeling and parameter uncertainty, and asymmetric information costs. The combination of a lack of basic data and complex modeling challenges result in very limited visibility into cyber risk. Without better cyber risk metrics, firms struggle to identify and address their cyber risk effectively, insurance providers hold back coverage, and governments lack visibility into potential systemic risks.

Over the course of the conference, panelists and participants identified a set of data and modelling needs for financial service firms. The discussions focused on 7 broad categories of cyber data needs:

1. Standardized definitions and a common language
2. Likelihood data
3. Loss/Impact data
4. Benchmarks against peers
5. Effectiveness of controls
6. Industry cyber risk models
7. Reporting metrics & frameworks for governance boards
Some of this data already exists within firms, but it is not currently shared in industry collaborations due to the sensitivity of the data. In other cases, data on risk models is not sensitive, but there are no existing venues for collaborating on cyber risk models.

An industry call for collaboration on cyber risk

Industry participants made a strong pitch for industry collaboration to solve the data and modeling gap, particularly when it comes to cyber risk definitions, metrics frameworks and models. Several of the speakers and participants in the conference highlighted how there is no competitive advantage when it comes to measuring cyber risk and that incidents affecting one firm have a negative impact on all firms. Many firms do their own data collections and model building in silos, so there is a clear opportunity to combine efforts and build definitions and models together for the industry. Some statements from industry leaders during the meeting include:

| “There is no competitive advantage in risk measurement and models” | Nedim Baruh  
| | JP Morgan |
| “We need to collectively work together or individually we will fail” | Mahi Dontamsetti  
| | State Street |
| “If one of us has a bad security day, then we all have a bad security day” | Nicole Clement  
| | Bank of America |
| “There has never been competition when it comes to cybersecurity in the financial service industry and there never will be” | Jim Routh  
| | Former CISO |
| “Sharing risk appetites, KPIs and KRIs does not give away a firm’s competitive advantage” | Ryan Harris  
| | Federal Reserve Bank of St Louis |
| “The data the industry needs already largely exists in silos. We would all benefit from stitching it together” | Aly Farooqui  
| | IBM |

Building a cyber risk community

MIT will launch a cyber risk research community composed of industry, academia and government to develop cyber risk metrics, models, and measurement approaches to improve security in the financial sector. This community will be organized around a working group composed of a broad group of private sector, academic and public sector stakeholders whose mission will be to develop shared metrics and models focused on improving cyber risk measurement. There is a clear need for better cyber risk models and data, and several speakers urged the group not to lose the momentum we have. MIT will look to launch the community in early 2023.

MIT will also convene a yearly cyber risk conference in the fall that brings together industry practitioners, academics, and government policy makers to explore developments, review research, and improve modeling and data activities.