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

28 March 2024
On January 17-18, 2024, 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 400 experts from industry, government, and academia to discuss efforts to **measure and model cyber risk** across the financial system. Over the course of two days, participants discussed how cyber risk is increasingly viewed in the broader context of enterprise risk and how firms and governments can improve communication about threats and risk. Several speakers argued that risk models need not be overly complex. Modelers should instead put an emphasis on fundamental controls. Industry members and regulators called for more collaboration on research and risk analysis to collectively strengthen the defenses of the sector, improve resilience, and provide tools for firms to better manage their own risks.

**Strategic approach to cyber risk management**

Cybersecurity was originally the province of company IT departments and, later, chief information security officers alone. The speakers at this year’s conference highlighted the fact that cyber risk is moving under enterprise-wide risk management, necessitating engagement from various roles and groups at each firm. Financial service companies’ chief risk officers and board members emphasized how cyber is viewed through a business lens that requires financial framing and consideration of the broader impacts on the business. The financial services industry’s understanding of cybersecurity is expanding and adapting to include the vocabulary of risk and financial governance. Security operation teams are increasingly asked to frame their work to governance boards in quantified financial terms. Benchmarking is increasingly important as regulators and company boards of directors increasingly require comparison against an organization’s peers to enable better oversight; however, this is proving difficult to implement.

Expanding the scope of cybersecurity practices is beneficial because it can tap into proven strategies from well-established risk management approaches such as operational risk. At the same time, speakers were quick to point out that technical and operational cybersecurity decisions should remain with the operational teams that have the expertise, just as the pilot of an aircraft has the final say on safety in flight.

**Modeling developments**

The rapid evolution of cybersecurity challenges can only be managed through widespread information sharing. Participants emphasized that there is no need to overcomplicate models. While AI-driven cybersecurity risk has received a lot of attention recently, speakers said it is more important to focus on implementing fundamental controls, and these should be the primary inputs of existing models. Modeling results show repeatedly that firms should focus on implementing foundational controls and planning for contingencies.

In the insurance marketplace, there are two contrasting threats for underwriters. The first is cascading risk, where an incident in one domain causes a domino effect of impacts
across other domains. The second is “death by a thousand cuts,” where many small claims overwhelm an insurer. Until these two threats become more manageable, the price of cyber insurance premiums will be high for limited coverage. Some participants highlighted the potential for market pricing of cyber risk and called for more research in this area.

Regulatory issues

Several speakers discussed the challenge of managing third-party risk and the potential need for additional regulation of outside providers whose services underpin core sectors. Recent large-scale incidents, such as those stemming from the Log4j vulnerability, highlight how some risks are outside the influence of financial service firms. Even as firms achieve greater insight into and control over the risk in their own systems, the change of 3rd, 4th and “nth” party risk is a growing share of overall risk. Several speakers also expressed a desire for more regulatory harmonization across jurisdictions, both within the United States and around the world. Harmonizing reporting requirements could free up resources for other security needs, and there are significant opportunities for standardization across jurisdictions. Regulations also serve as a powerful baseline and minimum standard for sector security, and participants called for more discussions of what those baselines should include. Financial service companies must defend against the most capable threat actors putting increased priority on the public-private partnerships that provide threat information flow between financial firms and governments. In one direction, firms need up-to-date information about threat actors and vulnerabilities. In the other direction, firms have experience that could inform policymakers.

Collaborative research and risk analysis

Participants called for collaboration on research and risk analysis but remain cautious about sharing sensitive data. Some solutions put forward include collaborating to validate cyber risk measures and expanding the scope of joint data collection. Outside entities, such as insurance providers, have some of the best visibility and can also help strengthen security in the sector. Ultimately, more dialogue between firms and the government strengthens the collective defenses of the sector, improves resilience, and helps individual risk management.

Looking ahead

Cyber risk management has matured significantly since the previous conference in 2022. Third-party risk will remain a key challenge going forward since typical mitigations such as redundancy only protect against loss of service/access but cannot address other risk such as the exfiltration of data. There was discussion about new threats such as quantum computing, and while the feasibility of large-scale quantum devices is still being debated, firms acknowledged the need to be prepared for a post-quantum environment. Participants noted that new and evolving threats can largely be incorporated into existing risk models with little difficulty.
Market pricing of cybersecurity risk is emerging, with instruments such as insurance-linked securities and the potential for new instruments such as cybersecurity breach swaps. Markets need data to price risk, though, and both Jeff Gerlach of the Federal Reserve Bank of Richmond and Daniel Weitzner from MIT, both conference organizers, called on the group to work together over the next year and come back to the next conference with new data and shared risked models. To make this happen, MIT will launch a consortium of financial service firms to create models and metrics corresponding to a set of core cyber risks identified and prioritized by the group. Academics and risk modeling teams from banks will work together to develop a standardized set of indicators, models, and definitions for cyber risk to guide corporate governance and management, enabling senior managers, executives, and boards of directors to define risk appetite, measure progress internally, mark-to-market risk, and benchmark against peers.