



Chicago Fed Insights, February 2025

FMG Operational Resilience Seminar: Event Summary

By Emma Weiss

Financial Economics

On November 21, 2024, the Federal Reserve Bank of Chicago's Financial Markets Group brought together around 50 participants from financial market infrastructures, central banks, regulators, and industry associations for a half-day seminar on Operational Resilience in Exchange Traded and Cleared Markets. The seminar was held under the Chatham House Rule, with no press in attendance.

The conference kicked off with welcome remarks from FMG head Cindy Hull and featured a keynote speaker and two panel discussions. Todd Conklin from the U.S. Department of the Treasury gave remarks on the role Treasury plays in helping the financial sector through the operational incident response to prevent systemic impacts from such events. Don Byron of the Futures Industry Association moderated a panel discussion focused on three financial market infrastructures' frameworks for operational resilience. A second panel discussion moderated by Seung Lee of the Federal Reserve Board of Governors explored financial stability implications of operational risk events and work being done at the national and international level to strengthen coordination and resilience. FMG policy advisor Ketan Patel gave closing remarks summarizing takeaways.

Several key themes emerged from the perspectives shared at the seminar.

- Operational risk is growing increasingly complex and requires firms to innovate and adopt more defensive strategies and engage in more scenario-based planning.
- Firms value making major investments in cyber risk prevention and mitigation, but there are some concerns about their ability to manage regulatory burdens associated with cyber risk management; small firms face additional challenges as they have lower capacity to finance robust cyber risk programs
- Financial sector third-party service providers play an important role in improving operational resilience, but can also introduce new vulnerabilities to firms.
- Cooperation between industry participants and entities in the public sector is critical for sharing information and coordinating responses to risk events to mitigate broader spillovers. A key policy area in which this plays out is around disconnect/reconnect protocols during operational or cyber incidents.
- Looking ahead, artificial intelligence (AI) has the potential to increase capabilities of cyber threat actors, as well as the potential to increase the ability of financial sector firms to defend against cyber attacks.

Evolving nature of operational and cyber risk

Conference participants discussed how the nature of operational risk is evolving in the face of increasingly aggressive cyber attacks and complex third-party service provider arrangements, the latter of which can both protect against cyber risk and be a source of risk. Multiple participants emphasized that over the past ten to 15 years, the importance of cyber and operational risk management has grown. Financial market infrastructures, such as clearing and settlement firms, are already highly regulated and subject to strong operational risk safeguards, but risk control self-assessments that previously were done on an annual or every two- to three-year cycle are insufficient. Firms now need to use information from service providers and clients to do more dynamic and timely risk assessments. As an example of this more expansive and involved approach, one senior executive from a financial services firm noted that instead of the approach used in prior years of operating from their backup site for a few hours, they now "fail over" operational activities for an entire month. They have also invested in the capability to rebuild their entire trading infrastructure "from bare metal" in a relatively short time frame.

A senior Treasury Department official outlined some of the increasing threats from nation-state actors that are subject to sanctions and thus have a heightened interest in attacking U.S. government and financial infrastructure and firms. He underscored the Treasury Department's attention to coordination and communication efforts to support increased resilience in the financial sector from these threats.

An official from the Bank of England shared insights on a new operational resilience framework published by UK authorities in 2022, focused on banks, insurers, asset managers, and financial market infrastructures. These firms were expected to work with all the financial regulators in the UK to identify the critically important business services without which the financial system could not operate and then engage with their users to understand the maximum level of disruption they could tolerate to those services. The UK is moving toward this type of model that identifies firms' maximum tolerance for disruption rather than setting timing goals like a two-hour recovery window. He noted these conversations about operational risk frameworks are happening in the international space as well, citing the example of the CPMI-IOSCO principles for financial market infrastructures.

Innovation and investment in defense against cyber attacks

Participants offered some examples of ways their firms are innovating and investing in preventing cyber attacks. As one participant said, "no one is going to cheap out on cyber." A chief risk officer of a large CCP noted that in recent years his firm has cut the time to patch vulnerabilities from seven to two days, and their firm is in the process of decommissioning legacy technologies that do not offer sufficient protection from cyber risk. Another CCP's business information security officer described the cyclicity of his firm's cybersecurity framework: They are using a systematic approach to continually assess their cyber maturity model across business areas, allocating resources toward business areas not meeting standards, and engaging senior management in a way that does not lead to more vulnerable business areas being penalized.

Representatives from both industry and government talked about how important public and private sector cooperation has been, with U.S. government agencies, including the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security and Treasury, providing threat intelligence feeds and critical vulnerabilities that firms, and especially smaller firms that don't have similar resources, can use to defend against cyber attacks. CISA also provides a cyber hygiene scanning tool that scans banks' public endpoints for critical vulnerabilities; this has been particularly useful for smaller banks.

The senior Treasury Department official mentioned that one downside of increased attention on cyber resilience has been an increased regulatory burden on firms. He suggested consolidating the number of cyber exams impacting a firm via better collaboration and coordination amongst the regulators. He also noted a downtick in ransomware attacks affecting the financial sector in the past few months after "hardening" in the sector, alongside an increase in attacks in other sectors. He foresaw a future in which the financial sector, in part because it is heavily regulated, could be "the core nucleus of a broader multi-sector response process" to cyber attacks.

Third-party service providers (TPSPs)

Participants noted that financial sector firms are increasingly reliant on technology solutions from TPSPs, which can provide increased efficiency and innovative technology. However, TPSPs embedded in financial sector firms' business functions and meant to protect against cyber and operational risk can also become a source of that risk themselves, as seen in the example of the CrowdStrike risk event in the summer of 2024. Additionally, financial sector firms can develop critical dependencies on such firms, which can be exacerbated by consolidation in the industry as successful firms are bought up by larger TPSPs. Participants emphasized the importance of having a diversified vendor supply chain. They also underscored how firms should understand their own critical dependencies and know what types of connections they have with each firm.

Attendees discussed different jurisdictions' regulatory regimes for TPSPs to the financial sector. The senior Treasury official observed that U.S. regulators hold financial sector firms to a higher standard than they hold the TPSPs on which the financial sector relies. He noted the Bank Service Company Act, which is the main vehicle that federal regulators have to examine TPSPs, is extremely limited in scope. Participants noted that recently some large provider firms have significantly improved their approach to resilience, speculating that perhaps this may be partly motivated by their desire to avoid being subject to more regulation and potentially being deemed systemically important.

Some participants contrasted the U.S. approach to that of the UK, where financial authorities have in fact brought some TPSPs under more direct supervisory oversight. In the past year, the UK Financial Conduct Authority, the Prudential Regulatory Authority, and the Bank of England have issued final rules on critical third parties, allowing the Ministry of Finance to suggest that certain critical third-party suppliers come under this regime. The regime will apply high-level regulatory principles to them and give the Bank of England and other regulatory authorities more information gathering powers, as well as enabling them to require scenario tests and participation in financial sector-wide scenarios. This regime has an emphasis on a financial stability perspective and leaves to the regulated firms the more micro issues, such as

identifying which services a firm is dependent on and what are their backup plans. One participant noted that the UK is modernizing incident reporting and taking steps to make financial market firms' reporting of third-party incidents more automated.

Incident response and the need for robust coordination and communication

Seminar participants noted that incident response is critical, given the evolving nature and threat from cyber attacks and the complexity of the financial sector supply chain and third-party relationships. Participants noted the importance of cooperation, communication, and coordination between the public and private sectors in this space. The senior Treasury official described how over the past several years he has worked with two umbrella bodies in the financial sector to strengthen their roles as risk management and response bodies for the financial sector. Specifically, these efforts have occurred in both the Financial Services Sector Coordinating Council (FSSCC), an industry group with over 70 members that coordinates the sector around critical infrastructure, cybersecurity, and resilience, and the Financial and Banking Information Infrastructure Committee (FBIIC), an analogous organization consisting of federal and state financial regulatory bodies. Important outcomes of this effort have been rapid communication sharing across the sector and a public communication process to help calm markets during a cyber or other major operational risk event that is systemic in nature. These umbrella bodies used their playbooks for the first time during the 2023 ION disruption, in which ION was subjected to a ransomware attack that disrupted its provision of derivatives trading and settlement services. In their view, they were able to contain the damage from that and other risk events.

Similar to the role Treasury plays in the U.S. across the financial sector, the Group of 7 (G-7) also has developed their capacity for rapid information sharing and response to cyber or operational incidents. For the CrowdStrike incident in mid-2024, for example, information received by U.S. officials from other G-7 official sector contacts allowed U.S. officials to have an understanding of the issue and a communication response prepared before U.S. financial markets opened—to prevent further knock-on financial stability effects. This official noted that in the future, the financial sector could potentially be the nucleus of a rapid response to an issue across the economy because of its heavily regulated nature and progress in developing these response protocols.

In reflecting on the successful communication in that event, one participant noted that they learned through a tabletop exercise the importance of basic preparations, such as having email distribution lists in place. Participants agreed that information sharing regarding operational and cyber threats and incidents was critical and benefited the sector as a whole.

Disconnect/reconnect considerations

An important area discussed at the seminar that affects both incident response and third-party risk management and brings together the public and private sectors was the protocol around disconnecting and reconnecting in the face of a cyber event or other operational disruption. According to participants, a key lesson learned from the ICBC ransomware attack in 2023 was that each firm has their own process for disconnecting and reconnecting, and that the decision on how that happens belongs to each firm and is based on their own risk management approaches. At the financial system level, whether national or global, more progress is needed to determine how to coordinate an orderly disconnection and reconnection process for a critical asset.

Some noted difficult trade-offs in the decision to disconnect or reconnect between cyber security risk and broader risk decisions. One participant noted their firm would likely resist pressure to reconnect from other participants or official sector bodies if the firm deemed it was not ready.

A senior official from the Bank of England also walked through their scenario testing, which recently explored an unexpected full financial sector shutdown and restart. He noted that the exercise consisted of around 750 people and included nonbanks and FMIs to account for interconnectedness in the financial sector. The exercise made clear the importance of filtering information and clear and timely communications for making decisions around disconnecting and reconnecting in a coordinated manner.

Looking ahead at AI

The use and evolution of artificial intelligence in operational and cyber risk was a key future consideration discussed by participants. All participants agreed that AI is still in early phases in terms of applications in this sector. Participants noted that AI by the attackers on offense could make cyber threats more potent: For example, deepfakes, disinformation campaigns, or viruses written by AI could be more difficult to detect or could possibly be used to break traditional encryption techniques. On the other hand, AI could be used by financial firms to help detect anomalies and reduce the number of false positives when scanning for malicious code as types of defense against cyber attacks. Additionally, adoption of AI could have

different impacts on financial sector firms by size. Larger financial institutions with large amounts of data can apply AI tools data to help them detect fraud. Meanwhile, smaller institutions may not be able to invest in AI to reap benefits, which could put further pressure on consolidation in the sector.

Conclusion

This FMG operational resilience seminar convened representatives from financial market infrastructures and the official sector across the U.S., UK, and Europe for an in-depth discussion on operational resilience. Participants shared first-hand experience gained from working to prevent operational risk events, including cyber risk events, from becoming financial sector-wide threats. They also discussed ways to mitigate risks from threat actors and strengthen resilience related to third-party service providers. FMG will continue to support work related to operational resilience of the cleared ecosystem.

Opinions expressed in this article are those of the author(s) and do not necessarily reflect the views of the Federal Reserve Bank of Chicago or the Federal Reserve System.