



Chicago Fed Insights, February 2025

Strengthening Operational Resilience in the Cleared Ecosystem

By Cindy Hull

Financial Economics

In November 2023, a ransomware attack on a U.S. subsidiary of the Industrial and Commercial Bank of China brought cyber risk into sharp relief for those who centrally clear financial transactions, especially on the heels of the cyber attack earlier that year on the Dublin-based ION financial trading services group.

The very high visibility of these risk events—and the resultant temporary payment interruptions—made them the cyber attacks that surely launched a thousand tabletop exercises aimed at improving operational resilience in the clearing ecosystem.

It's important to be clear about the stakes: Massive financial volumes flow through the clearing system. Its many firms helping to clear and settle transactions fairly and efficiently are vital to the execution of financial contracts made by entities ranging from banks to corporations to commodities producers.

At the Federal Reserve Bank of Chicago, these risk events spurred the Financial Markets Group of researchers that I lead to host a seminar on the topic of cyber risk, held the following November. And as we planned for that event, three key ideas for strengthening the resilience of operations in the cleared ecosystem came into focus.

In brief, they are: the importance of good translators across platforms, the need for wide coordination during and even ahead of crises, and the value of learning through experience in policy research.

We are in a new era of operational risks—whether we are adapting to innovations like AI, guarding against a cyber event, or navigating the uncertainties from the ever-growing set of technology-focused third-party service providers. But against that increasingly complex backdrop, I see these three ideas serving us well.

Regarding translators, I can remember times when I was on an operational team and, in the midst of a heavy trading day, learned that the SWIFT messages that convey critical transaction details to the counterparty didn't go through properly. Or the credit check process failed. Or a server decided to stop serving for a few moments.

It's probably normal to feel lost, queasy, perhaps a little panicked that this glitch will cost your client money and harm your reputation.

But with good translators in place, there can be quick resolution to such challenges, because they know how to speak each other's language. In a firm with good resilience practices, you may often see that otherwise large problems are quickly resolved because, say, a highly experienced trader talks to an equally experienced technology team member. They are able to quickly figure out what's causing the problem and then devise and implement a workaround.

Even on non-emergency days, skilled translation is vital to smooth trading operations. Technology, of course, brings speed and efficiency, but it also creates complexity and potential new dangers—including a seemingly mundane one, such as an upgraded trade execution platform that doesn't know how to talk to a legacy accounting system.

Resilience simply becomes more robust when firms have people who can translate between the two worlds of technology and operations. This leads not only to safe and efficient business-as-usual processes, but also to the ability to problem solve when a risk event occurs.

Translation is, in a sense, coordination. But I specifically want to emphasize the need for a broader kind of coordination during risk events—and in preparing for them.

When people in my group talk to market participants about their responses to cyber events, we sometimes hear that firms adopt a “disconnect first, ask questions later” mentality.

That approach—stepping back abruptly on a sliver of information—bears an eerie resemblance to the behavior of firms in the interdealer money markets at the onset of the Global Financial Crisis in 2008.

In that era, rumors about liquidity issues caused firms to quickly pull away from trading with one another, regardless of the veracity of the claim. This led to more rapid contagion and deeper damage.

When concerns over operational risk issues result in such sudden and drastic responses, it is a reminder that systemic implications of operational risk remain on par with those stemming from credit risk and liquidity risk.

At the same time, identifying, monitoring, and managing operational risk based on foreknowledge or forecasting is messy.

Managing operational risk is largely about doing the less glamorous stuff ahead of time: having robust procedures and business continuity plans, ensuring proper staff training, conducting fire drill exercises, and navigating vendor management programs.

These days it also requires wider-scale coordination—yes, even with business competitors. Perhaps especially with business competitors. For individual firms to really button down their own risk management practices in this ever more complex era, they have to conduct more coordinated planning and resilience exercises with a wide net of firms.

It’s important, even vital, to know what’s in each other’s playbooks. And it is heartening that so many firms are already participating in industry-wide and global central counterparty fire drills on a regular basis. For the sake of the system at large, the reach of such drills should be broadened.

Finally, I want to mention the third leg in my resilience stool, the importance of policy researchers in this area learning through experience. I know to a lot of people in the financial markets, research is as exciting as a forced software update. Even some researchers probably feel that way at times.

But in the era of operational risk I’ve been describing, those of us on the research side need a full quiver of operational approaches so that our work will better understand and anticipate the threat to financial stability posed by operational risk.

Doing the right analysis may not be only about data and regressions and formulas. We should also be making network maps, talking to people in the trenches across trading, clearing, and settlement, and learning from industry tabletop exercises. We can even get out of the office and watch operations in progress.

Operational risk events are never just one firm’s problem, especially in the cleared ecosystem—where a relatively small number of firms dominate each part of the trade lifecycle, from initiation through settlement.

This concentrated interconnectedness underscores why it’s so important to coordinate and communicate within and across firms and deeply study operational risk issues to better understand their potential threat to financial stability.

Doing so may help us identify potential trouble spots in the clearing ecosystem—whether from a large international trading firm or a widely used technology service provider—so that we can minimize broader threats to the system as a whole when the next disruption occurs.

Cindy Hull is the head of the Federal Reserve Bank of Chicago’s Financial Markets Group. This article is adapted from remarks she gave at Operational Resilience in Exchange Traded and Cleared Markets, a November 21, 2024, seminar sponsored and hosted by the Chicago Fed.

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.