**ICI VIEWPOINTS**
November 24, 2025

# Examining Broader Resiliency Challenges Beyond Traditional Cybersecurity Threats

Authors:

Andrew Kayiira

**2025 ICI Operational Resiliency Tabletop Exercise After-Action Report**

Read the report

Major service outages in internet-connected services are in the news and popping up in error messages on our screens with increasing, and alarming, frequency. The latest, in November 2025, saw an outage at global internet infrastructure and cybersecurity company Cloudflare reportedly caused by a bug in a routine update that had wide-ranging effects, even for consumers and businesses who aren't directly Cloudflare's customers. This has been growing increasingly common.

- On a Friday in July 2024, American cybersecurity company CrowdStrike released a buggy patch for one of its software packages, bringing computer systems down worldwide.
- On a Monday in October 2025, an Amazon Web Services outage affected 2,000 or so companies worldwide, disrupting web functionality, internet-connected products, and major services like online shopping and airline travel.
- On a Tuesday in July 2025, CoreDataX, a data vendor serving the financial industry, reported a critical outage that escalated over three days, disrupting trade matching, corporate actions, and settlement processing at multiple key service providers.

Each of these was a costly error that required affected organizations to act quickly and decisively to mitigate the damage, sometimes on a massive scale. But one major difference between these examples is that the CoreDataX outage never actually happened—CoreDataX isn't even a real company. This scenario was the focus of a

simulated tabletop exercise organized by ICI, designed to prepare member organizations for the realities of a world where an outage at a single company can cause significant downstream effects beyond its own client base.

## Convening Expertise

ICI brought together 42 member firms and more than 50 participants for the 2025 ICI Operational Resiliency Tabletop Exercise. Planned and led by ICI and volunteers from its Operational Resiliency Committee, this program combined ICI's major function as a convener of our membership and our operational expertise to develop and test strategies for managing a major systemic crisis.

ICI's committees are composed of employees from member organizations who collaborate to share knowledge for the benefit of each organization, the industry as a whole, and the long-term investors whom ICI represents. These committees bring together industry experts to solve complex problems within each committee's scope and generate best practices and critical resources for member organizations.

## Prep for the Worst

Hosted by Charles Schwab in Denver, the exercise simulated a prolonged outage at the fictional AlphaPrime Trust Company, triggered by a failure at CoreDataX. Participants were asked to assume AlphaPrime supported their own firm. Over three simulated days, evolving scenarios challenged participants to maintain continuity, manage liquidity, coordinate communications, and protect client confidence.

The ability to bring competing members of every size together to contribute has long been one of the major strengths of ICI and an important factor in the industry's biggest wins and innovations. The expertise of ICI's own industry operations team is always available to members for complex issues like those raised in this exercise. And the eagerness of members to participate underscores their commitment to the safety and security of fund shareholders.

## Building Strength Across the Industry

The simulation presented opportunities for attendees to identify potential gaps in their resiliency planning and test their response strategies. This generated a wealth of insights and takeaways to strengthen member preparedness across legal, risk, compliance, operations, and technology functions.

By focusing on fourth-party risk—the risk introduced when a business depends on a service provider that has its own dependencies that may fail—the exercise moved beyond traditional cybersecurity threats to examine the broader challenge of operational resilience in a deeply interconnected industry.

## Commitment to Operational Excellence

Operational and systemic risk management is a concern for every industry, especially given the rapid pace of technological change. Service disruptions can take many forms and require multifunctional teams to manage.  These challenges often benefit from extraordinary cooperation across the industry for knowledge-sharing and contingency planning.

We encourage even more member organizations to participate in initiatives like this, enabling the industry to draw from a broader pool of skillsets and enhance overall preparedness. Sharing the critical findings from tabletop exercises like this one helps

strengthen the cybersecurity of the industry as a whole, ultimately benefiting individual investors.

---