

OPERATIONAL RESILIENCE

LME Week 2024

Breakfast Forum

Hamish Adourian

Head of Sales & Marketing, Sinara

Matt Dolton

CEO, Kynetix

14 October 2024

kynetix

Sinara
The trade engineering people

During LME Week 2024, senior operations leaders from trading firms, particularly within the metals futures sector, gathered for an insightful discussion on the current and emerging challenges of operational resilience. The forum, hosted by Sinara and Kynetix, was designed to foster an exchange of ideas and experiences, highlighting the importance of resilience across the business, not just IT. In this short report, we present a summary of the morning's key takeaways and insights.

Investment in Operational Resilience

One of the central themes was the need for **significant investment** in operational resilience across the business. While firms generally acknowledge its importance, securing the necessary funding can be challenging, particularly when it is seen as a “cost centre” rather than an enabler of continuity and growth. The conversation emphasised the importance of framing resilience in terms of its business value. For example, rather than discussing the technical aspects of system redundancy, firms should highlight how such investments protect revenue streams and reputation. Investment in resilience isn't just about risk management; it's about future-proofing the business.

Engaging Senior Management and Boards

Operational leaders often face the challenge of how to effectively **communicate the importance** of resilience to senior management and boards without overwhelming them with technical jargon. The consensus was that leaders should focus on articulating how resilience impacts business outcomes. Instead of discussing the nuances of a disaster recovery plan, the conversation should focus on how the lack of such a plan could lead to significant financial losses or regulatory penalties. For example, a downtime incident for a major trading platform could result in substantial missed trades and reputational damage, especially in a volatile market. As a result, the dialogue must evolve from “what can go wrong” to “how we can stay competitive and compliant by mitigating operational risks.”

Maintaining a Flexible Playbook

One of the most important points raised was the necessity of maintaining a flexible **incident response playbook**. No matter how comprehensive a business continuity or incident plan may be, it is impossible to anticipate every potential crisis. The conversation underscored that resilience planning should not focus solely on the last incident—future incidents are likely to arise from unexpected sources. Rigid response plans often don't work and need to be rethought on the fly. The lesson

here was clear: flexibility is a critical component of operational resilience.

Third-Party Vendor Resilience

With increasing reliance on third-party vendors, especially in areas like cloud hosting and outsourced IT, the discussion also touched on the importance of third-party vendor resilience. The challenge here is that while trading firms can control internal operations, they often have limited insight into their vendors' own resilience strategies. The key takeaway was the need to ensure that third-party vendors are integrated into a firm's resilience planning, with open communication, close collaboration between frontline application support teams, and clear expectations for incident response times.

Incident Response in Hybrid Work Environments

The shift towards hybrid working models has added new layers of complexity to incident response. Traditionally, incident response might have involved quickly gathering key operations staff and decision-makers in a room, but remote work has complicated this. The group agreed that ensuring the right people can convene quickly is essential for mitigating the impact of an incident. Firm need to ensure rapid communication and decision-making even when team members are scattered across

different locations. This shift towards virtual response plans was seen as a necessary evolution in today's work environment.

Cloud and Data Centres

Cloud technology and the use of datacentres were also prominent topics. The benefits of cloud infrastructure—such as scalability, flexibility, and cost efficiency—are well understood, but the group discussed the associated risks, particularly around security and resilience. A hybrid model, with a mix of cloud and on-premise solutions to ensure business continuity in the event of a cloud service disruption, was explored.

Backup Systems for Critical Functions

The debate around backup or secondary systems for critical functions generated a lively discussion. While backup systems can take over in the event of a primary system failure, they are not without their own challenges. The group considered both the benefits and drawbacks of maintaining secondary systems, perhaps using entirely different technology and infrastructure from the primary system. While they can offer continuity, they can potentially be costly and complex to manage. The last thing anyone would want is a backup system, which hasn't been adequately tested, failing when needed, causing further delays. This highlighted the importance of not just having backup systems but ensuring they

are tested, fit for purpose, and can quickly take over in the event of disruption.

Not Just Responding to the Last Incident

Finally, a key point was the danger of being overly reactive to the last incident, rather than preparing for the next. Several attendees shared experiences where teams were focused on resolving issues from a previous crisis, only to be blindsided by an entirely different type of disruption. The consensus was that resilience planning must be forward-looking and holistic. One firm shared their approach of running regular scenario exercises that force teams to think outside the box and prepare for less obvious risks, such as geopolitical unrest or supply chain problems.

Conclusion

In conclusion, the discussion underscored the evolving nature of operational resilience, particularly in the face of rapid technological changes and a shift towards hybrid working. It is clear that trading firms must continue to invest, adapt, and think ahead to both ensure robust operations and maintain a competitive edge.



Sinara have been operating at the sharp end of metals, commodities, and financial trading for more than 30 years, working closely with exchanges, brokers, and clearers to streamline, integrate and automate processes from order entry through to settlement.



Kynetix builds agile software for capital markets firms including banks, broker and exchanges. HelloZero, the award-winning post trade data automation platform, delivers control and trusted data quality.