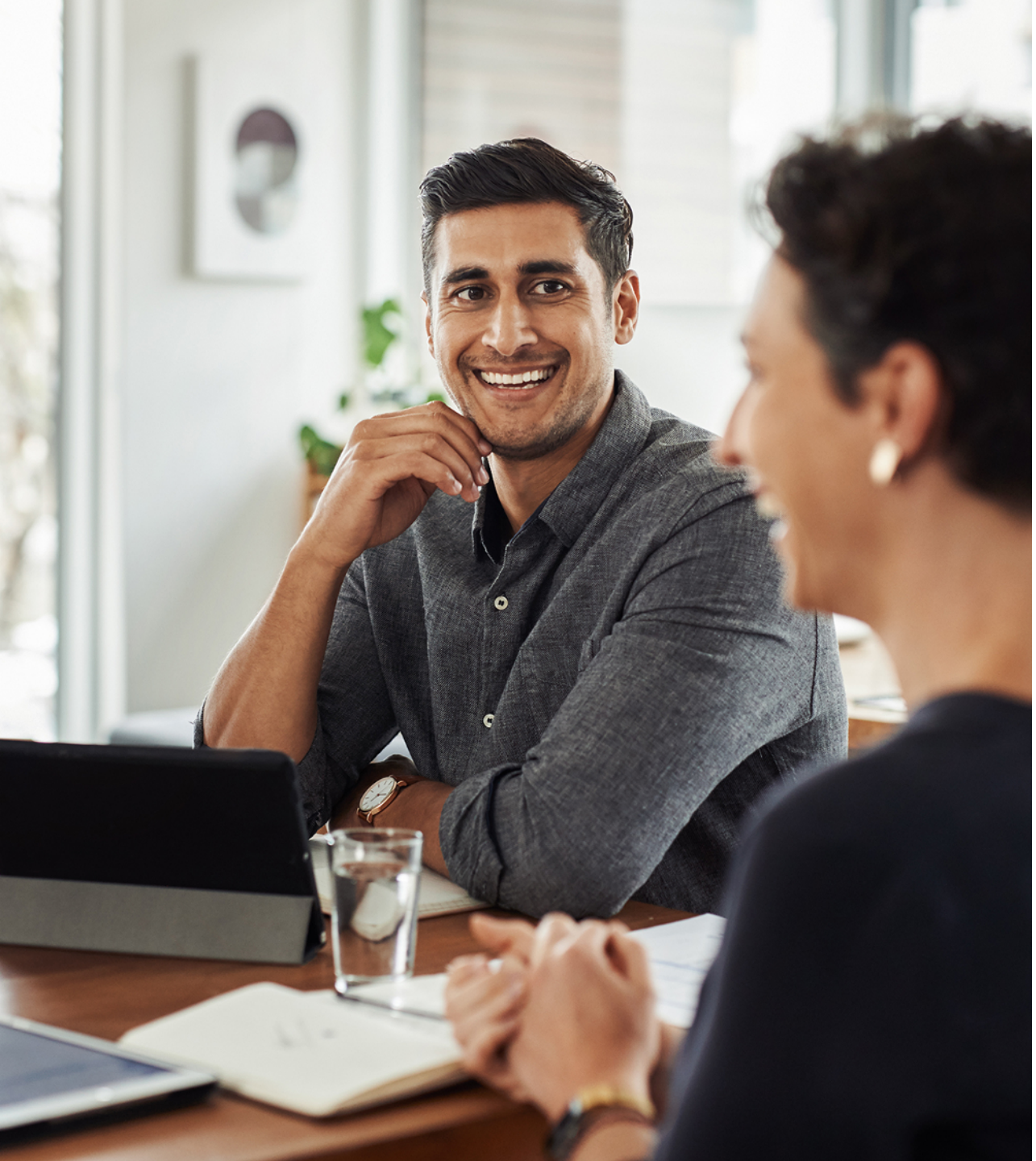
Executive Summary

Security and Resiliency Expert Exchange

March 24, 2026

kyndryl



Overview

During the Kyndryl Security and Resilience Expert Exchange, cross-industry security and resilience leaders engaged in a strategic discussion on the continuous evolution of enterprise resilience. The conversation highlighted how organizations are adapting to increasingly complex digital and geopolitical threats that extend well beyond standard regulatory requirements.

Host/SME

Conal Hickey
Cyber Resilience and Connectivity Leader, Vice President Kyndryl Strategic Markets

Jorgen Floes
Distinguished Engineer, Cyber Resilience and Connectivity Practice, Engineering Lead Kyndryl Strategic Markets

Key topics

The evolution of resilience beyond traditional security

- Enterprise resilience now demands that organizations move past basic digital protection and prioritize comprehensive service availability to ensure business operations withstand broader economic or physical shocks.

- Participants widely agreed that enterprise resilience must transcend standard digital protection to encompass customer stability, facility operations, and comprehensive financial solvency. A retail banking executive noted that executive boards increasingly expect security leaders to answer complex questions regarding overall corporate stability during cyber incidents, forcing technical teams to rapidly rethink their corporate roles.

- Leaders vigorously debated the specific terminology used to describe this evolution, with a leading industry executive championing the strategic concept of service integrity. By framing the objective as service integrity rather than security, organizations can more easily secure executive buy-in for funding strategic reserves rather than masking these critical efforts as mere cost-saving migrations.

- One member shared a best practice involving the rigorous reclassification of all corporate assets to determine baseline availability and integrity needs. By mapping specific business continuity controls strictly to these asset classifications, companies can avoid over-investing in low-priority systems while ensuring their most critical revenue-generating environments remain heavily protected from operational disruption.

"We cannot simply talk about security anymore; our core mission must focus on broader service integrity, revenue protection, and the continuous availability of our systems."

CISO Expert Exchange Member

Security and netwoks snapshot

Learn more

Managing third-party and supply chain risks amidst global uncertainty

- Evaluating and securing the supply chain is a highly volatile component of enterprise resilience, requiring leaders to navigate geopolitical conflicts, contract limitations, and the massive practical challenges of live recovery testing.

- One member highlighted the subjective and unpredictable nature of geopolitical risk by sharing a real-world supply chain dilemma. Their organization relocated a vendor from a sanctioned nation to a seemingly safe European island, only to face renewed operational uncertainty when an entirely unrelated geopolitical conflict subsequently impacted the new location.

- While participants agreed on the absolute necessity of testing vendor resilience, they diverged on the practical execution of these stress tests. A professional services representative questioned whether companies actually execute live recovery tests in production environments, arguing that the high risks and operational burdens make such clauses purely theoretical.

- Responding to the testing debate, a few members countered that regulatory pressure will soon mandate documented evidence of complex vendor resiliency testing. Conversely, one CISO admitted that neither their industry nor vendors currently possess the maturity to guarantee uninterrupted operations during severe crises, such as wartime personnel shortages.

- Another CISO expressed deep frustration with the limitations of regulatory frameworks, arguing that standardized risk assessments fail to account for unprecedented global crises. This participant stated that heavily consolidated industries cannot easily switch suppliers, rendering standard contractual exit clauses completely ineffective during a true disaster.

> “Life is much more difficult than the regulations; no standard contract can foresee or mitigate a crisis where half of a vendor's staff is suddenly called away to fight in a war.”
>
> CISO Expert Exchange Member

Why leaders need 360-degree cyber awareness in an age of instability

Learn more

Defining organizational ownership for resilience

- Companies are actively debating who should lead resilience efforts, as traditional security leaders find themselves tasked with managing enterprise-wide crises that fall far outside their core technical expertise.

- A resilience engineering expert challenged the group to identify who actually owns the corporate resilience agenda, noting that most global organizations still lack a dedicated executive for this specific function. Another CISO agreed with this subjective observation, sharing that their institution still relies on informal cross-functional committees rather than empowering a centralized resilience officer.

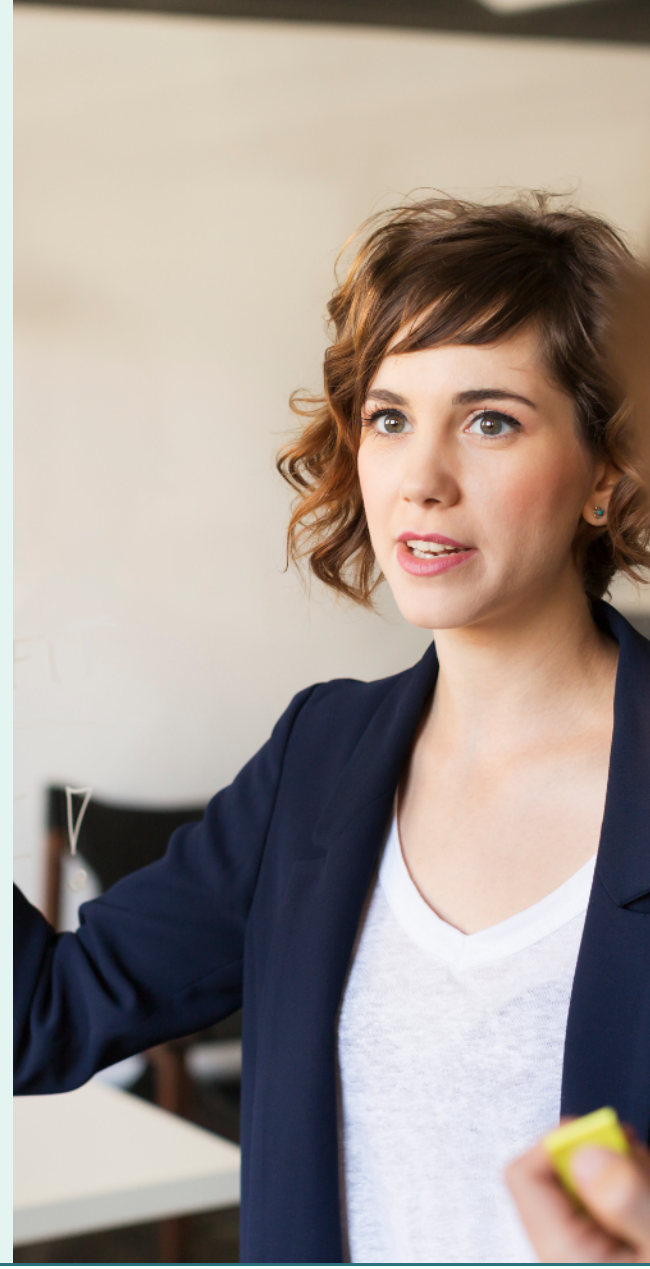
- One executive shared a successful best practice of establishing a monthly executive resilience committee to govern operations. This collaborative approach allows the security leader to act as a team captain who facilitates discussions, while ultimate accountability accurately remains with the chief operating or risk officers.

- Another member questioned whether security leaders should merely be temporary custodians of the corporate resilience mandate. They suggested that as new global business threats emerge and corporate structures adapt, this responsibility might eventually shift to entirely different corporate departments.

> "I am not the right person to talk knowledgeably about financial solvency and global energy markets, yet these critical questions increasingly fall to the security function."
>
> — CISO Expert Exchange Member

Master governance to enable innovation and minimize risk

Learn more



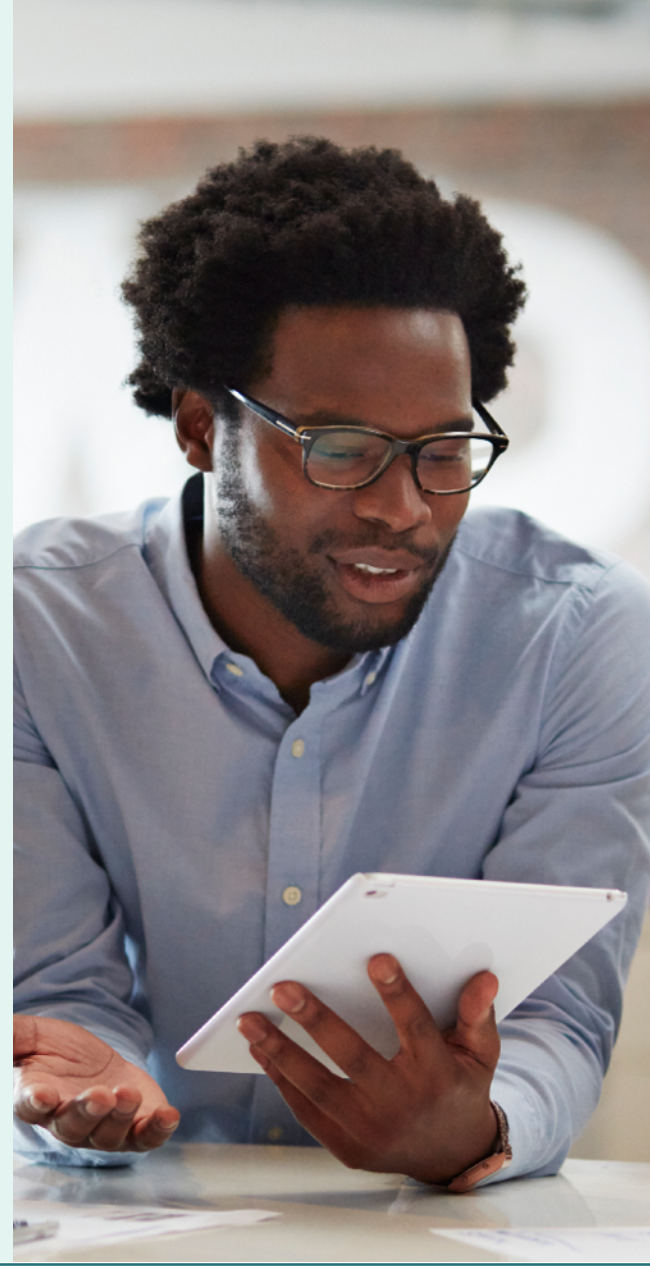
Operationalizing resilience and building anti-fragility

- Organizations must systematically embed resilience requirements directly into their product development and procurement lifecycles while striving to build corporate systems that actively improve under stress.

- A security architecture executive observed a widespread lack of foundational resilience planning among business units and product developers during the initial system design phase. To counter this dangerous negligence, they shared a best practice of embedding automated architectural recovery questions directly into the continuous product development pipelines, ensuring teams address operational recovery before launching products.

- A technology facilitator emphasized that actively reducing vendor fragmentation can actually improve overall system design and corporate stability. By standardizing operations onto a smaller number of critical platforms, organizations can focus their resilience engineering and testing efforts much more effectively across the entire supply chain.

> **"We need to go a step further than simply withstanding a disaster; we must learn from the crisis and deliberately design our companies to become anti-fragile."**
>
> **— CISO Expert Exchange Member**



kyndryl

The Security and Resiliency Expert Exchange is hosted by Kyndryl. Please contact Andre Putter or Wiem Sabbagh with any questions about Kyndryl or this exchange.