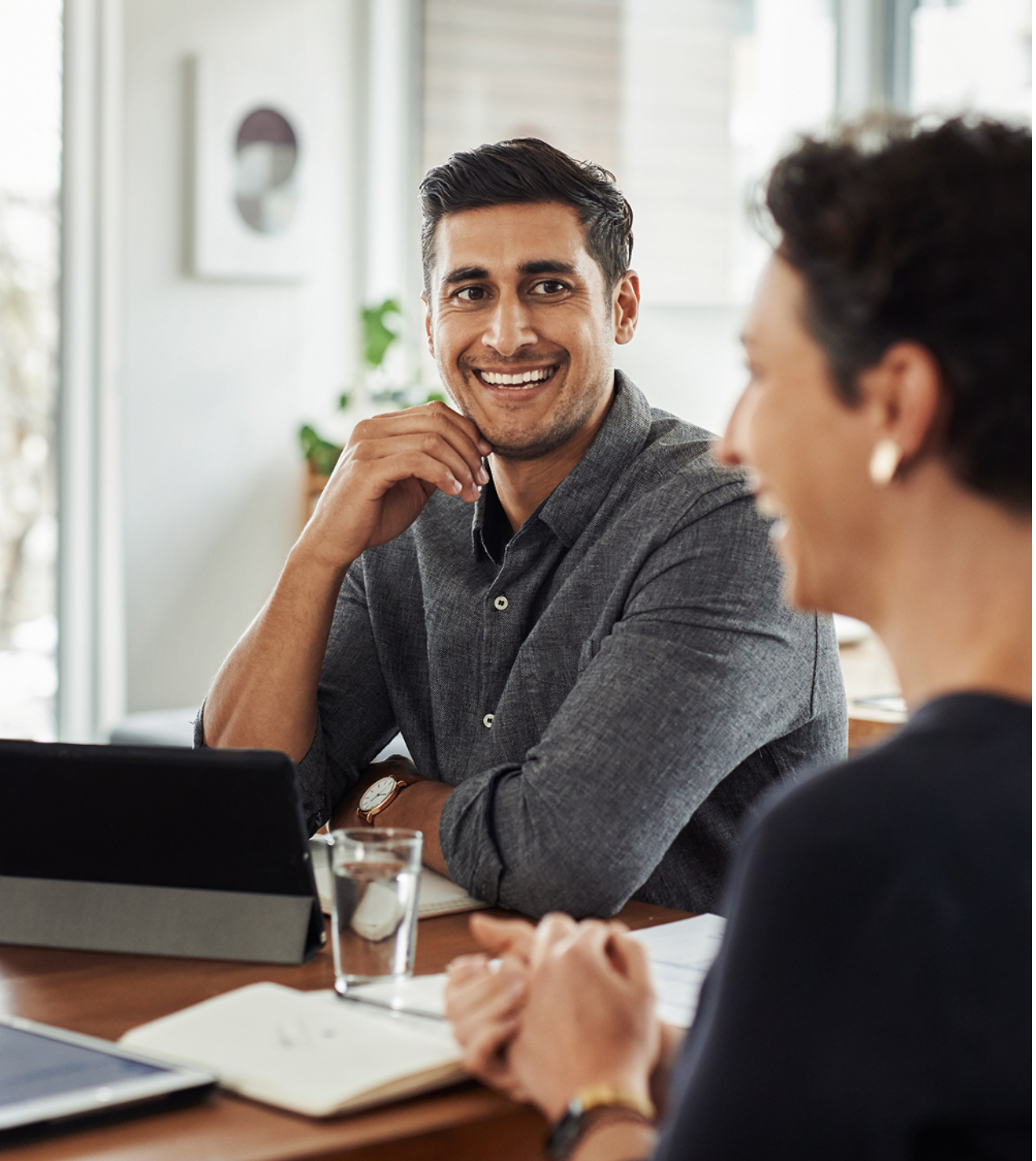
CISO Cross-Industry

# Expert Exchange

## Q1 Executive summary
January 22, 2026

kyndryl



# Overview

A group of cross-industry CISOs convened to discuss the shifting landscape of enterprise resiliency. The conversation moved beyond traditional IT disaster recovery to focus on holistic, business-centric strategies. Participants agreed that while technical recovery is essential, true resiliency requires the ability to maintain operations during significant disruptions, including cyberattacks and third-party failures.

# Host

Justin Haney
Kyndryl, US Vice President – Security and Resiliency

# SME

Allen Downs
Kyndryl, VP Security and Resiliency Services

# Key topics

# Resiliency Versus Disaster Recovery

- One participant observed that ownership is often fragmented across the enterprise, with responsibilities split between security officers and technology officers, creating governance gaps in which those accountable for recovery lack the authority to execute it.

- One retail executive defined resiliency as the combination of business continuity and disaster recovery, noting that while they are distinct functions, they must be synchronized under a unified oversight framework to be effective.

- A state government executive highlighted the communication gap between technical teams and business units, noting that security teams often define resiliency differently than operational leaders, who focus on mission completion rather than server status.

- One participant observed that ownership is often fragmented across the enterprise, with responsibilities split between security officers and technology officers, creating governance gaps in which those accountable for recovery lack the authority to execute it.

- Participants from the public sector emphasized that, for their agencies, resiliency often involves physical safety operations, such as traffic management, which require coordination with emergency response teams rather than just IT departments.

"Resiliency is a cross-enterprise capability expanding beyond disaster recovery. True resilience requires organizational alignment, clear ownership, and the ability to operate through distributions, not just restore systems after an incident."

— CISO Expert Exchange Member

Unblocking Cyber Resilience: The power of Mass Recovery Modeling

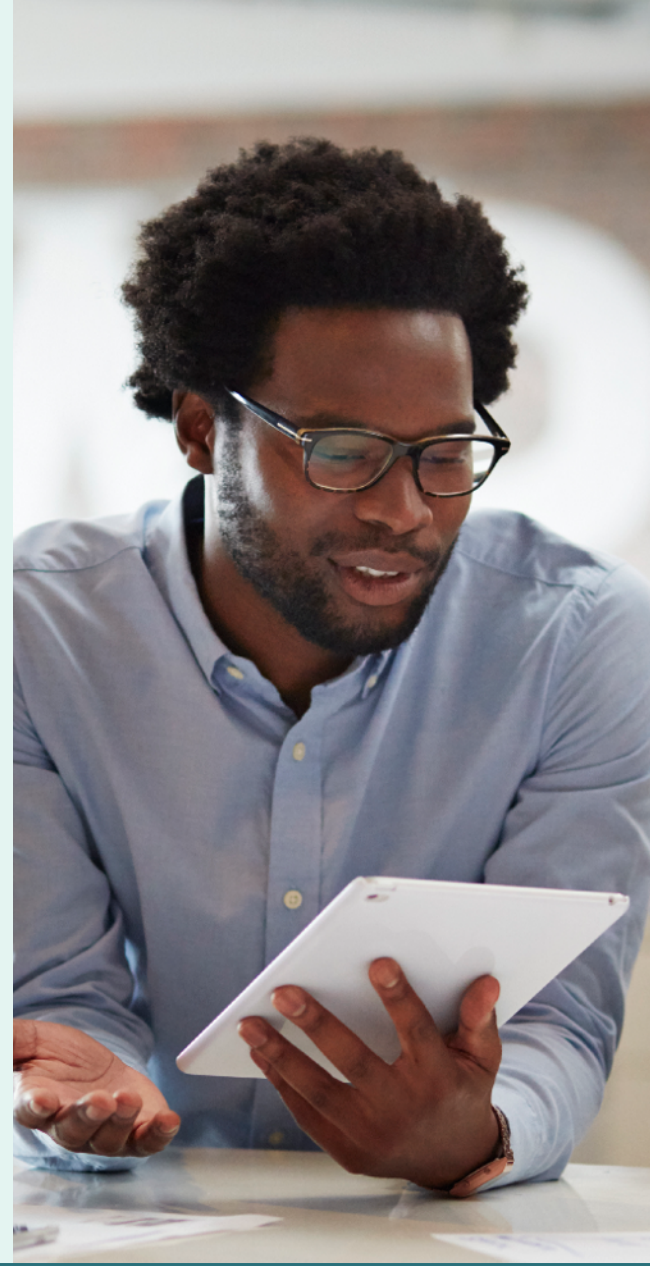
Learn more

# Managing Third-Party Risks

- The group identified reliance on external vendors as a significant vulnerability, emphasizing that vendor failure is often overlooked in internal planning and leaves organizations with few options.
- One executive noted the difficulty of managing risks when relying on major service providers, admitting that when a primary cloud service fails, the only option is often to wait for the vendor to restore service.
- Participants confirmed that vendor selection is often based on price rather than resiliency capabilities, warning that vendors who do not invest in their own recovery maturity pose a direct risk to the client organization.
- There was consensus that organizations must audit their supply chain's ability to support resiliency requirements, rather than assuming vendors will always be available to support business processes.

**"We have 40,000 assessments that we maintain from the resiliency side. Our vendor risk management program focuses on business continuity, partnering with the contract owners and vendors to document and test continuity plans for critical services, and prioritizing resources based on business impact."**

**— CISO Expert Exchange Member**



# Defining Minimum Viable Operations

- Executives stressed the need to identify “crown jewels” and non-technical dependencies to ensure the company can function during a digital outage, a concept referred to as the “minimum viable company.”

- A healthcare executive explained that critical dependencies often involve non-technical services, such as food or linen supply, urging peers to look beyond software when defining essential business functions.

- A manufacturing leader described an executive exercise simulating a two-week enterprise software outage, which forced leadership to determine how to process transactions manually and maintain a “minimum viable company” status.

- Based upon work with a variety of clients/industries, Kyndryl SMEs advised shifting from an infrastructure-centric view to a business-centric view, focusing on the financial impact of lost services rather than just the restoration of servers and applications.

- Participants acknowledged the difficulty of this approach, with one manufacturing leader admitting that determining how to survive manually during a long-term outage remains a tough, unsolved problem for many modern plants.

“In healthcare, business continuity means the surgeon must keep operating even if the IT systems go down.”

— CISO Expert Exchange Member

5 Strategies for Managing Third-Party Risk

Learn more

# Testing and Validation Strategies

- The conversation revealed a spectrum of testing maturity, ranging from standard tabletop exercises to physically disconnecting systems to force reliance on backup processes and manual workarounds.

- One manufacturing executive shared a proactive strategy where they disconnect the enterprise from the internet quarterly, forcing the business to rely on out-of-band communication and manual shipping processes. This aggressive testing approach required significant stakeholder buy-in, but leadership accepted it because they understood the potential implications of failing to contain a real security event.

- Another manufacturing participant suggested inviting personnel from different plant locations to observe tabletop exercises, encouraging them to proactively think about resiliency for their own unique environments.

**"On a quarterly basis, we pull the enterprise off of the internet, forcing the business to operate in isolation and validate their ability to continue core operations like orders, planning, and shipping, while ensuring the security team is prepared to act decisively if needed."**

**— CISO Expert Exchange Member**

kyndryl

The CISO Expert Exchange is hosted by Kyndryl. Please contact Justin Haney with any questions about Kyndryl or this Exchange.