

Resilient operations: Four practices for attacks at AI speed

Insights from the October 2026 CISO Expert Exchange

kyndryl

Contents

01 Cyber resilience

02 Response authority

03 Resilience baseline

04 Third-party risk

05 Decision authority

06 What is the Kyndryl CISO Expert Exchange?

07 Kyndryl cyber resilience services

01

How to plan for cyber resilience

On October 22, 2026, Kyndryl hosted a cross-industry US CISO Expert Exchange to explore security issues emerging with frontier AI and how organizations are responding. Participants from technology, manufacturing and US state and local government identified a growing gap between the speed of AI-enabled attacks and the pace of enterprise decision-making. What does this mean for resilience planning?

Organizations need to test resilience before an incident, bringing technology, business operations, suppliers and decision-makers into the same scenario to expose dependencies, decision gaps and recovery issues before a real disruption.

The discussion surfaced four practices that Kyndryl believes are central to frontier-AI readiness:

- Pre-authorize critical response decisions
- Define and test the minimum viable company
- Govern suppliers according to operational criticality
- Use tabletop exercises to establish decision authority

How Frontier AI is reshaping risk



02

Pre-authorize critical response decisions

AI-enabled attacks expose a structural mismatch between automated offense and human-paced defense. While AI can help defenders analyze threats and accelerate remediation, many response actions still depend on fragmented tools and lengthy approval processes. The strategic need is to create an operating layer that can connect signals, apply business context and act within defined boundaries at high speed.

The most consequential roadblock is decision authority. Participants emphasized that vital actions, such as isolating networks or shutting down production systems, should not require real-time executive approvals during an active incident. Instead, organizations should establish clear decision thresholds in advance, defining when security teams can act autonomously and what assets they must act to protect first. At the same time, organizations must balance rapid remediation with operational stability, recognizing that rushed patching can introduce new risks to critical business systems.

“We patched 3,000+ instances in 45 minutes, with only two websites going down. That kind of speed comes from having the tools and the authority to act before a crisis hits.” — Tech Industry Participant

Outpacing risk: Security readiness for the AI era



03

Define and test the minimum viable company

Good resilience planning means figuring out how the company will continue operating during an extended disruption. Participants stressed that the minimum viable company extends beyond technology recovery alone. Manufacturing, service delivery and customer interactions may need to continue while critical systems are unavailable.

Extended-outage exercises, recovery drills and direct engagement with business units frequently reveal dependencies that conventional resilience documentation can miss. Such dependencies include paper-based procedures, disconnected medical devices and manufacturing instructions, and legacy systems. Technology teams responsible for restoration and business leaders responsible for sustaining operations must share accountability for the process of discovering and validating these dependencies.

“The question is not ‘How quickly can an application recover?’ but ‘How does the company operate while the application is unavailable?”

— Manufacturing Industry Participant

How an insurer strengthened resilience and simplified IT



04

Govern suppliers according to operational criticality

Participants agreed that traditional third-party risk programs often fail to reflect the true importance of suppliers to business operations. A vendor that supports a mission-critical process may be affected by deep dependency chains that can obscure operational vulnerabilities. The result is aggregate risk: a hardened enterprise can lose a critical capability because its supplier lacks sufficient resilience to cyber threats.

"I do not care if I'm paying you 10 bucks. If it is germane to me being in business, you are an important vendor."

— Tech Industry Participant Executive

Repeated supplier risk transfer:

→ Diversify / Replace / Exit
→ Greater resilience
→ Greater ecosystem complexity
→ Optimize supplier footprint
→ Fewest suppliers needed to sustain critical operations

CISO takeaway:

Reduce dependency without increasing complexity beyond what resilience requires.



05

Tabletop exercises decision-making authority

Executive tabletop exercises provide an opportunity to rehearse leadership decisions before a real crisis Executive tabletop exercises provide an opportunity to rehearse leadership decisions before a real crisis occurs. Participants agreed that decisions about ransomware payments, operational shutdowns, public communications, legal responses and recovery priorities should not be improvised during an incident.

Participants suggested that 90-minute exercises tend to be most productive, particularly when legal, communications, business and board stakeholders participate alongside security and technology teams.

The scenario and intent matter most; these sessions should help clarify governance responsibilities, expose conflicting assumptions and reinforce the distinction between oversight and operational management.

> “The primary value of executive tabletops is establishing clear decision-making authority and political alignment before an actual crisis occurs.” CISO Expert Exchange participant



Why layered controls are essential for governing AI agents

06

What is the Kyndryl CISO Expert Exchange?

The Kyndryl CISO Expert Exchange is a curated, peer-driven program that brings together CISOs and senior IT leaders for meaningful collaboration and shared learning. There are CISO Expert Exchange communities in the U.S., Canada and Europe.

The October 2026 conversation was moderated by Justin Haney, Vice President, Practice General Management, Kyndryl.



Justin Haney
Vice President, Practice General Management, Kyndryl

Visit Kyndryl CISO Expert Exchange



07

Kyndryl cyber resilience services

Kyndryl helps organizations transition from their current infrastructure to a high-performance, AI-native future. Our security and resiliency services are designed to accelerate growth and innovation, offering scalable solutions that protect data and AI assets, ensure compliance, and stay ahead of emerging threats. We secure mission-critical infrastructures and develop AI-native capabilities by combining strategic advice with hands-on execution, empowering leaders to confidently pursue growth and innovation. Learn more at Kyndryl.com.



kyndryl

© Copyright Kyndryl Inc. 2026. All rights reserved.

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.