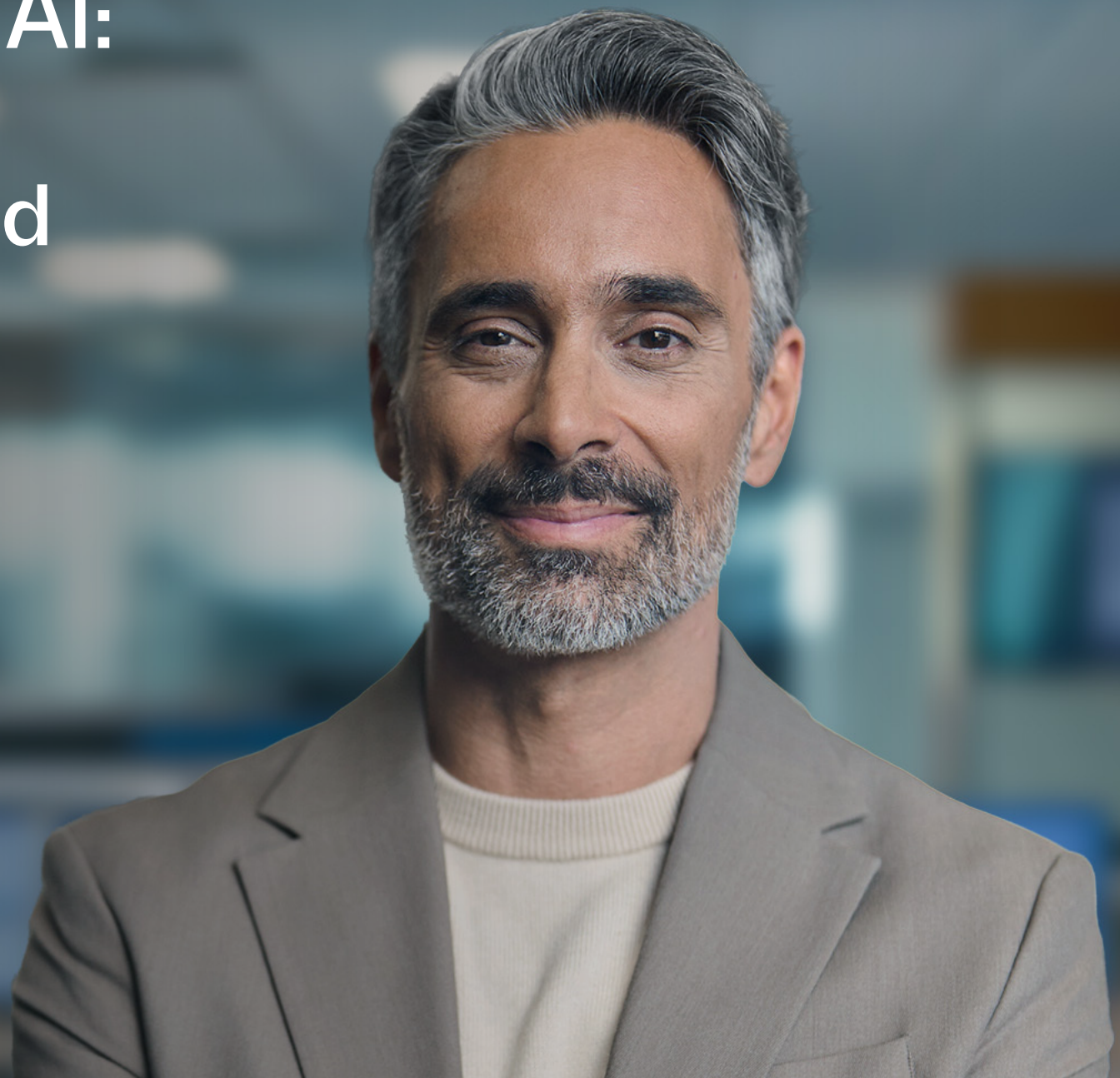
Resilience for frontier AI: Four priorities for enterprise security and IT professionals

Insights from the October 2026 CISO Expert Exchange



kyndryl

Contents

01
Cyber defense and resilience - one discipline

02
Long-term resilience

03
Minimum viable operations

04
Judge severity scores

05
Govern AI adoption

06
What is the Kyndryl CISO Expert Exchange?

07
Kyndryl cyber resilience services

01

Cyber defense and resilience as one discipline

Frontier AI is intensifying long-standing weaknesses in how enterprises manage vulnerability and approach governance. **Security leaders see the need to shift from treating cyber defense and resilience as adjacent disciplines to managing them as two sides of the same operating model.**

On October 15, 2026, Kyndryl hosted a Security & Resilience Expert Exchange to explore these issues and generate ideas and best practices for approaching them. Fifteen participants joined the wide-ranging conversation.

The discussion surfaced four priorities:

- Embrace short-term disruption to allow for long-term resilience
- Define and prove the minimum viable operations
- Judge severity scores in business context
- Govern AI adoption to enable innovation while mitigating risk

How Frontier AI is reshaping risk



02

Priority 1 : Embrace short-term disruption to allow for long-term resilience

AI is enabling faster vulnerability discovery, but patch speed is not a sufficient standalone security metric. The practical question is how much short-term disruption the organization is prepared to accept to reduce the probability of a longer, more damaging outage. A patching program that closes findings quickly but repeatedly interrupts essential processes is not resilient, but preserving uptime by deferring every difficult change leaves the organization exposed.

Leaders described the need to set a clear appetite for controlled downtime and test whether critical services can move to an alternate infrastructure without advance preparation. The strongest programs use the urgency around frontier AI to elevate existing resilience work, including backup modernization, recovery testing, application-landscape monitoring and the automation of patch testing.

"We are going to see shorter bursts of downtime in order to prevent the longer runs of downtime from an unmitigated patch." –Participant working in the banking



Outpacing risk: Security readiness for the AI era

03

Priority 2 : Define and prove minimum viable operations

The concept of a minimum viable company is becoming the practical center of cyber recovery, and minimum viable operations must be engineered and proven end-to-end. Organizations must understand the full sequence of infrastructure, identity, data, application, network, DNS and third-party dependencies required to restore critical services after an enterprise-wide loss of IT.

This means that recovery planning must move away from isolated systems toward complete business processes. This requires current dependency data, protected recovery environments, verified data integrity and clarity on whether recovery targets depend on hot standby, cold restore or a third location. Continuously checking data for anomalies before placing it in a quarantined third location is imperative. Regulation is helping formalize this discipline, particularly for European financial institutions operating under DORA and ECB scrutiny.

“This is where we need to start to think about business processes rather than an application.” Participant working in the banking industry.



04

Priority 3 : Judge severity scores in business context

Prioritization is a core resilience capability in a world where AI models can surface potential weaknesses faster than defenders can validate them and release fixes. Generic severity ratings remain useful, but they do not show which exposures are reachable, connected to a critical service and actively exploitable. Instead, leaders need a shared decision-making model that weighs exploitability, operational impact, recovery readiness and customer consequences.

Teams can prioritize remediation based on real exposure by using a digital twin of the environment, which combines vulnerability data with the asset inventory, NDR, EDR, SIEM and other telemetry. Simulation, including Monte Carlo analysis, can identify which significant vulnerabilities are most consequential in the organization's own environment. This approach concentrates limited patch windows and engineering attention on the most business-critical exposures. Where immediate patching is unsafe or unavailable, organizations are expanding the control set with segmentation, modernization, virtual patching, attack-surface mapping, preventive controls, enhanced detection and faster response.

"What we need as organizations is to determine which of those vulnerabilities are actually going to get us on the 9:00 news." –Participant working in the banking industry



05

Priority 4 : Govern AI adoption to enable innovation while mitigating risk

Leading enterprises are reframing security as an enabler with guardrails instead of a roadblock. Cybersecurity should work directly with innovation teams to offer approved technologies in secured environments. Governance committees should assess whether proposed AI projects deliver meaningful enterprise value before they advance.

Responsible AI governance, controlled development environments, open-source component checks and formal risk acceptance can guide tool selection without creating an approval bottleneck. In application development, deployment can be prevented when critical or high vulnerabilities remain unless an authorized management function explicitly accepts the risk. Chief executives and board directors are increasingly involved in cyber-resilience decisions, both around budget and on governance questions about risk appetite, operational disruption and the ability to move at business speed. Tabletop exercises can make those trade-offs tangible, expose weaknesses and clarify that resilience depends on coordinated ownership across silos.

"The more we innovate with AI, the more exposures we create." –Kate Yamashita, VP, Global Security and Resilience Consult Lead, Kyndryl

Why layered controls are essential for governing AI agents



06

What is the Kyndryl CISO Expert Exchange?

The Kyndryl Security & Resiliency Expert Exchange is a curated , peer-driven program that brings together senior IT and security leaders for meaningful collaboration and shared learning. There are Security & Resilience Expert Exchange communities in the U.S., Canada and Europe. Participation is open to CISOs and senior security executives from large enterprises.

Insignts and observations in this report are derived from the October 2026 Security & Resilience Expert Exchange. These findings are intended to reflect emerging patterns and peer perspectives rather than universal benchmarks.

The October 15, 2026 conversation was moderated by Conal Hickey, VP Kyndryl Strategic Markets, Cyber Resilience and Connectivity Leader . Its Kyndryl subject-matter expert was Kate Yamashita, VP, Global Security and Resilience Consult Lead, Kyndryl.



Conal Hickey
VP Kyndryl Strategic Markets, Cyber Resilience and Connectivity Leader



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.