Executive Summary

Thought Leadership Exchange for Financial Services

June 2, 2026

kyndryl

Overview

The Thought Leadership Exchange is a Kyndryl-hosted, international peer-to-peer community for senior financial services technology leaders to share challenges, exchange insights, and benchmark against peers on critical industry issues.

In this session, participants examined how increasingly capable AI models are accelerating the discovery and exploitation of software vulnerabilities, compressing remediation timelines, and driving increased regulatory attention and, in several cases, heightened board-level focus across European banking and insurance institutions.

Host

Stewart Hyman
Kyndryl, Chief Technology Officer for Strategic Markets

SME Guest

Conal Hickey
Kyndryl, VP Security & Resiliency

Key topics

Frontier AI as an Inflection Point for Vulnerability Management

- Frontier artificial intelligence models are emerging as a significant inflection point for cyber defense, discovering software vulnerabilities far faster and in far greater volume than existing tools and challenging how the industry prioritizes remediation.

- Frontier AI models surface substantially more vulnerabilities than traditional scanning approaches. As one example discussed, a widely used codebase was cited where earlier model versions identified only a small number of vulnerabilities. In contrast, newer frontier models identified several hundred in the same code that had been in circulation for years. The underlying vulnerabilities are not new, but these models locate them far more quickly and easily. Also, comparable capabilities are likely to emerge across both proprietary and open-source tools, making this a broader industry shift rather than a single-vendor phenomenon.

- Discussions uncovered that frontier models can combine multiple low-severity vulnerabilities into a single critical attack vector, challenging the conventional practice of prioritizing remediation solely by published severity ratings. A Kyndryl perspective proposed shifting to a risk-based approach that considers the criticality of affected assets and the minimum viable systems required to operate the business. This approach resonated with several participants.

- Organizations will need to "fight AI with AI," embedding greater automation into cyber defense and zero-trust controls while prioritizing the protection of their most critical assets.

- Participants identified managing their primary vendors' suppliers as a significant compliance hurdle. Companies acting as intermediaries must review every downstream subcontract to ensure regulatory adherence. As a result, financial institutions are implementing stricter criteria to limit the number of officially classified critical vendors.

- One perspective pointed to industry projections indicating a sharp rise in vulnerability remediation, with some estimates suggesting up to a 50% increase in patches over the next 12 to 18 months. At the same time, participants highlighted that attackers may be able to exploit vulnerabilities much faster than before. That said, there was also cautious optimism that as these same models become more widely used in code testing, they could ultimately help strengthen overall software security.

"AI amplifies both risk and opportunity—accelerating the discovery and impact of vulnerabilities while equally strengthening our ability to anticipate and defend against them."

— Conal Hickey,
VP Security and Resilience, Kyndryl

Secure your enterprise for the Frontier AI era

Start here

Accelerating Patch Cycles Across Process and Tooling

- Several leaders reported pressure from regulators and, in some cases, from their boards to compress patch cycles from weeks to days or even hours. Participants broadly noted that process constraints, rather than tools limitations alone, are often the primary barrier.

- Some described situations in which supervisory authorities and management boards have requested updates on readiness posture, placing patch velocity firmly on the executive agenda for some organizations. Others indicated that this level of attention varies by institution and market.

- Release testing and approval processes are frequently the main bottleneck. Participants noted that adopting faster tools delivers limited benefit if approval workflows remain unchanged. As a result, organizations are exploring ways to streamline or selectively automate testing processes while maintaining confidence in release quality, particularly for customer-facing applications.

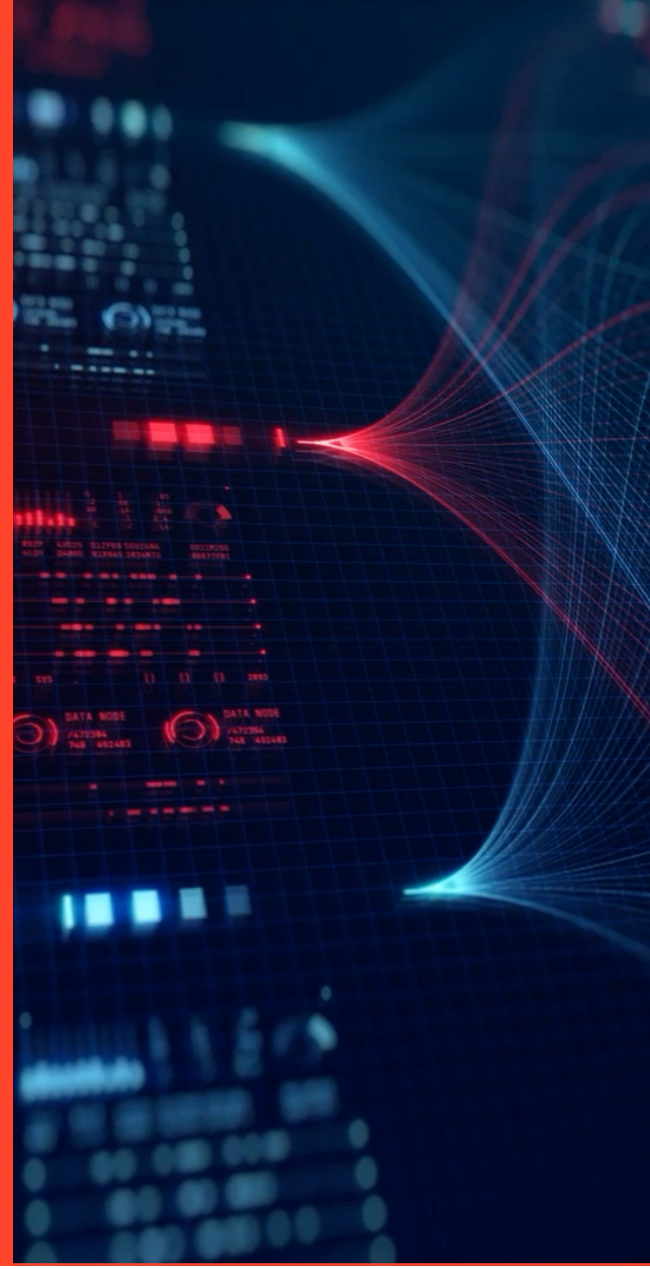
- Participants described the use of dedicated readiness squads to address the increased pace of remediation. These teams focus on automation opportunities, risk prioritization, and compensating controls—particularly for legacy or unsupported systems. Examples included efforts to increase patch frequency through automation of operational processes such as system shutdown and restart.

“Don’t wait for the vendors — focus on whether your processes are ready to absorb a tool that can go faster, because that’s where the real constraint lies.”

— Stewart Hyman,
CTO Strategic Markets, Kyndryl

Kyndryl Agentic AI Framework

Learn more



Building Cyber Resilience and Regulatory Readiness

- Cyber resilience is increasingly seen as a foundational requirement for organizations operating in a digital environment. Participants discussed investments and approaches to ensure the ability to sustain and recover critical business processes regardless of incident type.

- Participants described increased regulatory engagement, with several organizations reporting direct requests from supervisors and joint supervisory teams for visibility into their readiness posture. One perspective highlighted ongoing discussions within European regulatory bodies that may lead to further policy tightening and accelerated preparedness timelines.

- Kyndryl representatives observed strong and growing interest among clients in resilience solutions such as isolated recovery environments, immutable storage, and clean copies of infrastructure separated from production. Participants also emphasized the importance of foundational practices, including regular validation of backup and recovery capabilities and implementation of compensating controls around legacy systems.

- Cyber security-related investment cases are, in many instances, receiving strong support from boards, particularly where linked to regulatory expectations and emerging risk from frontier AI.

"Having a clean copy of your digital infrastructure, protected and separated from production, is really becoming required to protect you fully."

— Conal Hickey,
VP Security and Resilience, Kyndryl

Benchmark your cyber resilience against AI-driven threats

Learn more

Modernizing Legacy Estates and Governing Agentic Development

- Participants described ongoing modernization efforts, with several noting an acceleration aimed at enabling faster patching and improved resilience. Modern architectures—particularly containerized environments—were seen as better suited to rapid remediation than traditional virtualized environments.

- Discussions highlighted two parallel priorities: strengthening resilience measures while progressively modernizing legacy applications. Participants shared experiences using AI-driven tools to reverse engineer and document legacy code, with particular complexity noted in environments heavily dependent on database-resident logic and interdependent stored procedures.

- Some organizations reported that their most progressive teams have adopted agentic development extensively. In these cases, developers increasingly use AI to define architecture, plan work, run development tasks, and generate code for review. However, maturity levels varied significantly across organizations, with some teams still in earlier stages of their adoption journey.

- Participants also raised concerns about rising token costs associated with AI usage, noting that managing cost efficiency is becoming an important consideration. Approaches discussed included using different models for different types of tasks, applying governance guardrails, and implementing usage limits.

- The group generally sees artificial intelligence as an amplifier of developer capability rather than a direct replacement, emphasizing the importance of maintaining human expertise and oversight. Governance was identified as a critical factor, particularly in controlling how AI tools are used beyond developer environments. While agentic coding by experienced developers was broadly supported, several participants indicated that autonomous AI agents with access to sensitive or production data remain out of scope until stronger controls are established.

- One perspective also introduced the concept of a trust-based maturity model for AI autonomy, highlighting that progression from human-in-the-loop systems to fully autonomous operation is likely to take place over an extended period and will require robust measurement, auditing, and governance.

"Since Claude came along, many of our top developers haven't coded a single line for months. They use it to define architecture, plan work, execute tasks, and generate pull requests, often switching between different models for advanced analysis and execution within their cloud environments."

— FSS Expert Exchange Member

Beyond code conversion:
An AI-led approach to modernization driving business outcomes

Explore

kyndryl

The FSS Leadership Exchange is hosted by Kyndryl. To learn more or to become a member of this community, please connect with Stewart Hyman on LinkedIn or email at stewart.hyman@kyndryl.com.