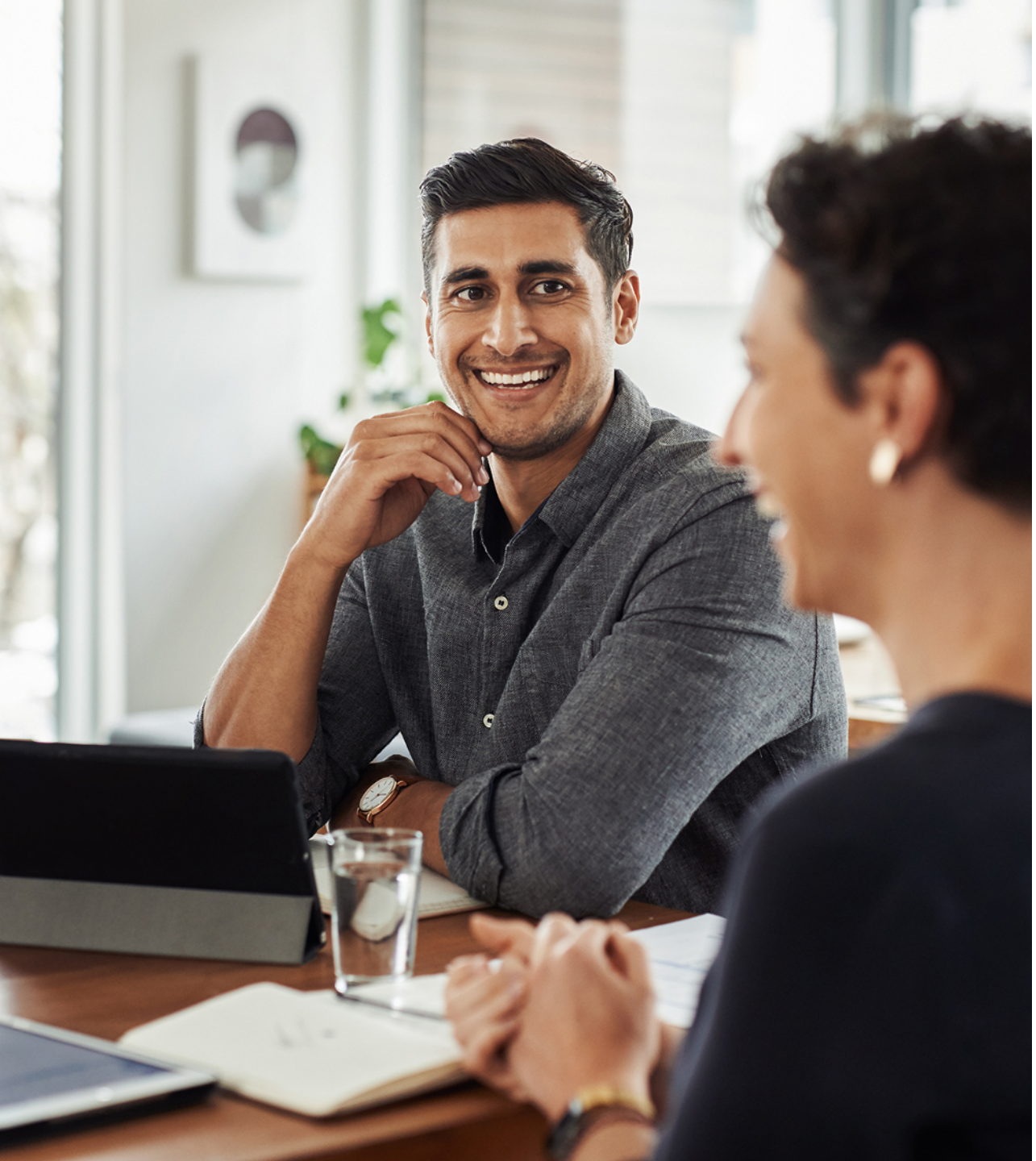
Executive Summary

# Security and Resiliency Expert Exchange

June 24, 2025

kyndryl



# Overview

In the Kyndryl Security and Resiliency Expert Exchange held on June 24, 2025, senior CISOs Exchange members from a diverse mix of countries and industries convened to discuss topics of significant interest concerning security and Artificial Intelligence (AI).

Key discussion areas included, benefits and risks of AI deployment, AI governance, protection against AI threats, and AI's role in enhancing security.

# Host


**Conal Hickey**
Vice President
Security and Resiliency, Kyndryl

**Jorgen Floes**
Vice President
Security and Resiliency, Kyndryl

**Anthonie De Bos**
Vice President
Security and Resiliency, Kyndryl


# Key topics

# Navigating AI Governance and Deployment

- The demand for new AI tools is predominantly business-driven, as organizations increasingly seek to harness the power of AI to drive rapid business value, leading to uncontrolled adoption.

- Organizations are actively exploring AI governance frameworks, transitioning from initial uncertainty to understanding basic needs like application inventory, employee training, and awareness. One participating member is considering NIST as a framework for AI implementation.

- A crucial step in AI deployment involves selecting enterprise-approved AI tools, with Microsoft Copilot one of the frequently chosen tool, due to its information protection capabilities and seamless integration within existing Microsoft ecosystems. To manage user adoption, organizations provide workshops and sessions on the “dos and don'ts” of public AI tools, emphasizing the necessity of a governance concept around their usage.

- Some members have established centralized AI teams or centers of excellence to identify opportunities, define standards, and manage AI topics. However, internal challenges such as inconsistent data quality can hinder the effectiveness of AI tools.

- For external AI tools, existing cloud application workflows are often applied. Organizations treat external AI tools similarly to any cloud application, focusing on managing associated with data privacy and security concerns. The process involves formal requests and checks by various departments, including infrastructure, business, procurement, and compliance.

- Companies are attempting to standardize technology and centralize the evaluation of these demands. They often face challenges in managing high-quality, relevant data, particularly regarding accuracy, reliability, and completeness. One participant suggested preparing an internal resource, such as a checklist, to guide users based on data criticality. Ultimately, the consensus pointed to a need to focus on and standardize a few approved tools to manage complexity and risks effectively.

> “One of the main challenges for us lies in educating users on how to safely use AI. Most cannot judge the risk to the organization. The use of company computers, prompts that may house sensitive data, making sensitive data public. There is a need to work on awareness perspective.”
>
> — Kyndryl Security & Resiliency Expert Exchange Member

**Cybersecurity at a historic inflection point: Navigating the converged threats of digital age**

**Learn more**

# Addressing AI-Related Security Risks

- A primary concern is the uncontrolled proliferation of AI usage by employees. If clear guidance and policies are not in place, it will lead to “Shadow AI” that is difficult to detect and control.

- Data confidentiality and privacy are paramount, especially when sensitive data might be used with public AI tools or shared with third-party AI models. One opinion is that third parties do not always prioritize security, noting that “no code low code” solutions often imply “no security”.

- All participants agreed sharing data with third parties and AI models must be taken seriously. This necessitates efforts to better understand and classify data and implement data security posture management to prevent critical data from being shared with AI models. While EU AI Act mandates training requirements for users, though awareness and implementation vary among CISOs.

- The increasing sophistication of AI-driven threats, such as advanced phishing emails and deep fakes poses significant challenges. One participant raised concern about identifying fraudulent activities when AI emulates voices, stating, “if bad actors leverage AI emulating the voice of our CEO, not many will think the call is fraudulent”.

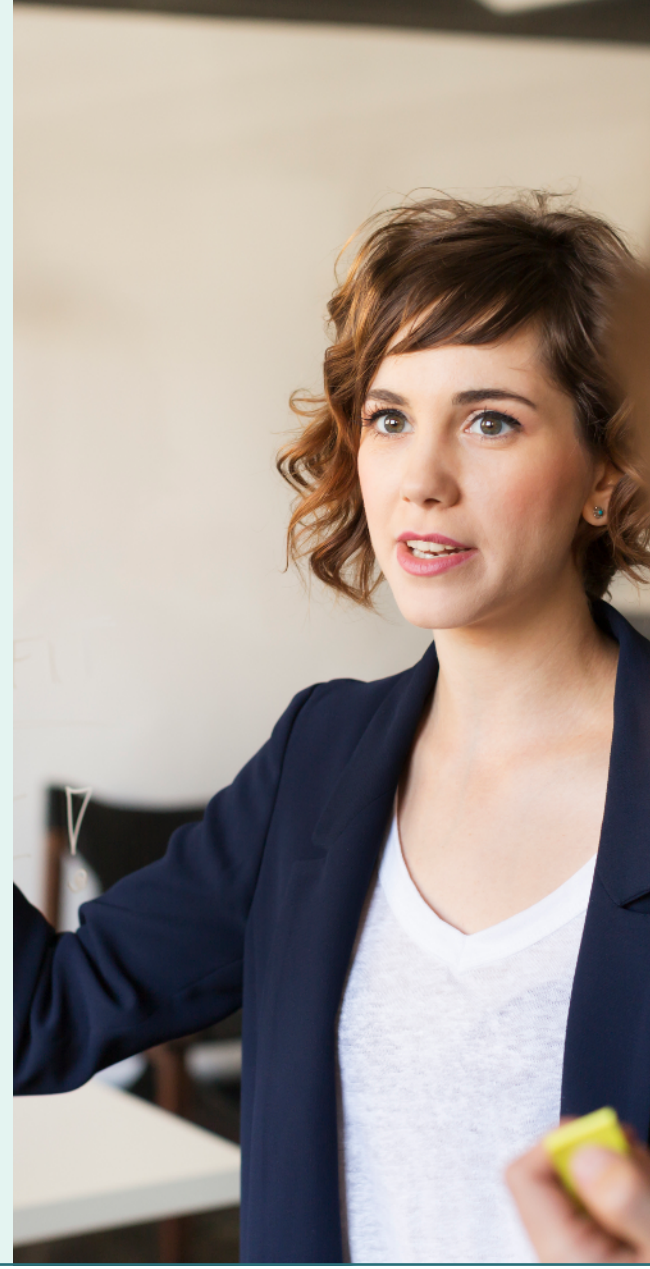
- There is a critical need for better data classification to determine which data criticality levels allow the use of specific AI tools. Tony DeBos from Kyndryl highlighted new technological protections are emerging, such as tools that create AI gateways to control AI activities and prompt security tools that protect prompts and scan for vulnerabilities.

**“It's a hype moment and the business is trying to find productivity through these investments.”**

**— Security and Resilience Expert Exchange Member**

**Three focus areas to improve security for AI projects in 2025**

**Learn more**



# Leveraging AI for Enhanced Security Operations

- Some organizations are adopting Microsoft Copilot to make Security Operations Centers (SOCs) more efficient. One CISO explained how they are using Copilot in incident investigation, identifying impacted devices, and responding to zero-day vulnerabilities.

- AI is also being explored for full automation stacks, including the automated isolation of clients and scanning for AI-generated malware. This shift is driven by the rapidly evolving cyber threat landscape, where hackers are automating attack steps like scanning, vulnerability exploitation, and reconnaissance using AI. A participant cited a recent simulation where a full ransomware attack was executed in less than 25 minutes using AI.

- Rapid evolution of AI necessitates security teams to "loosen the brakes" for adoption of defensive measures, automating responses, and moving towards more proactive management, even if it causes minor disruptions. "Automatic locking of accounts that are suspected to be compromised" was one of the suggestions. Jørgen Floes from Kyndryl mentioned an example of AI being used for advanced detection, such as identifying fake voices in service desk calls to prevent unauthorized access.

- Adoption of agentic AI is not yet a core strategic driver for all companies, it is recognized as being on the cusp of mass adoption within the next one to two years.

- Based on the expert exchange, a critical strategic recommendation for senior leadership teams is to prioritize and accelerate the development of a holistic AI data governance strategy. This strategy must explicitly address comprehensive data classification across all organizational data, the implementation of advanced Data Loss Prevention (DLP) solutions tailored for AI, and the establishment of clear, enforceable policies for both internal and third-party AI tool usage.

**"It's one of the more challenging areas. It's important to know how your critical third-party providers are running their operations, right? And if you think about the application development, and application co-development that's done — how are they managing security when they're doing that co-development?"**

**— Security and Resilience Expert Exchange Member**

**Modernizing for the AI era: A blueprint for readiness**

**Learn more**

kyndryl

The Security and Resiliency Expert Exchange is hosted by Kyndryl. Please contact Conal Hickey with any questions about Kyndryl or this Expert Exchange.