CISO Cross-Industry

Expert Exchange

Q2 Executive summary
May 13, 2025

kyndryl

Overview

Business executives and security leaders from various organizations convened to discuss the evolving landscape of data security, particularly in the context of Artificial Intelligence integration. Participants shared insights on navigating the complexities of data classification, access management, tool effectiveness, balancing security with business needs, and establishing clear data ownership.

Host

Justin Haney
Kyndryl, USA Vice President –
Security and Network Leader

SME

Kris Lovejoy
Kyndryl – Global Security and
Resilience Practice Lead

Key topics

Evolving Data Security Strategy in the Age of AI

- The advent of AI is fundamentally changing how organizations approach data security, prompting a re-evaluation of traditional strategies that focus on data discovery, monitoring data egress, and protection through masking or encryption.

- Participants discussed how the traditional three-pillar strategy—knowing what data exists, tracking data leaving the company, and ensuring data is protected—needs adaptation. One executive noted that the rise of AI requires considering new dimensions for securing data.

- A key concern highlighted is the integrity of data used for AI training, particularly when sourcing external data feeds. While some organizations trust the integrity of data provided by third-party services, others focus on managing the integrity of their internal data fed into AI systems.

- AI provides a powerful force multiplier for malicious actors, allowing them to rapidly process vast amounts of leaked or scraped data, making internal data protection significantly more critical than ever before. This increased risk underscores the need for stronger data protection measures.

- One executive noted that the availability of powerful tools that can connect diverse data sources more effectively drives increased focus on data security. These tools enable faster deployment of data-driven initiatives, increasing the potential impact of data on the organization.

- Another perspective offered was that AI enables businesses to sift through and derive value from vast amounts of historical data, prompting a greater focus on ensuring data quality and security for effective use by these new tools.

> “Do the same [data security strategy] pillars make sense today, or is there a new dimension designed to secure data?”
>
> — CISO Expert Exchange Member

Challenges in Data Classification

- Executives acknowledged that a substantial amount of existing data is not correctly classified, leading to either over- or under-protection. The manual classification process for large datasets is a major challenge. There is significant interest in exploring how AI can be leveraged to automate or improve data classification accuracy, moving beyond reliance on human judgment that can be inconsistent over time. Better classification is seen as a prerequisite for adequate protection.

- Implementing a model of least privileged access, where individuals only have access necessary for their role, is an aspiration but is considered difficult to achieve in practice. Organizations are working towards this goal despite the implementation complexity.

- Tools that can provide fine-grained access control based on user identity and data sensitivity are being evaluated and piloted.

> "How do you get to a model where you have released privileged access, so people only have access to the data they need to do their job? This is gains efficiency to say, not so gains efficiency to implement."
>
> — CISO Expert Exchange Member

Balancing Security Controls with Enablement

- Organizations face a critical balancing act between implementing necessary security controls to protect data and enabling the business to use new technologies, particularly AI, for productivity and innovation.

- A key tension exists between security measures, sometimes perceived as inhibiting business activities, and the imperative of businesses to use data and AI for success and competitive advantage.

- Security leaders strive to protect and monitor data without blocking business functions, seeking solutions to enable safe productivity. The focus is on facilitating the effective use of AI while managing security risks.

- Strategies enabling AI use while maintaining security include deploying internal-only AI tools with limited initial access and developing policies and guardrails before wider deployment.

- Some organizations use a coaching-based approach rather than strict blocking for accessing external AI tools, using security solutions to warn customers about policy violations and monitor sensitive data usage.

- Executives discussed the challenge of sorting through the hype surrounding AI capabilitiesto determine which tools genuinely offer business value, allowing for a more balanced discussion about the security trade-offs involved.

> “How do we use AI to be more productive while being safe? I'm not looking to block it or prevent it. Instead, I'm looking to use it and see how we can do that most efficiently and effectively without the security implications.”
>
> — CISO Expert Exchange Member

kyndryl

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

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.