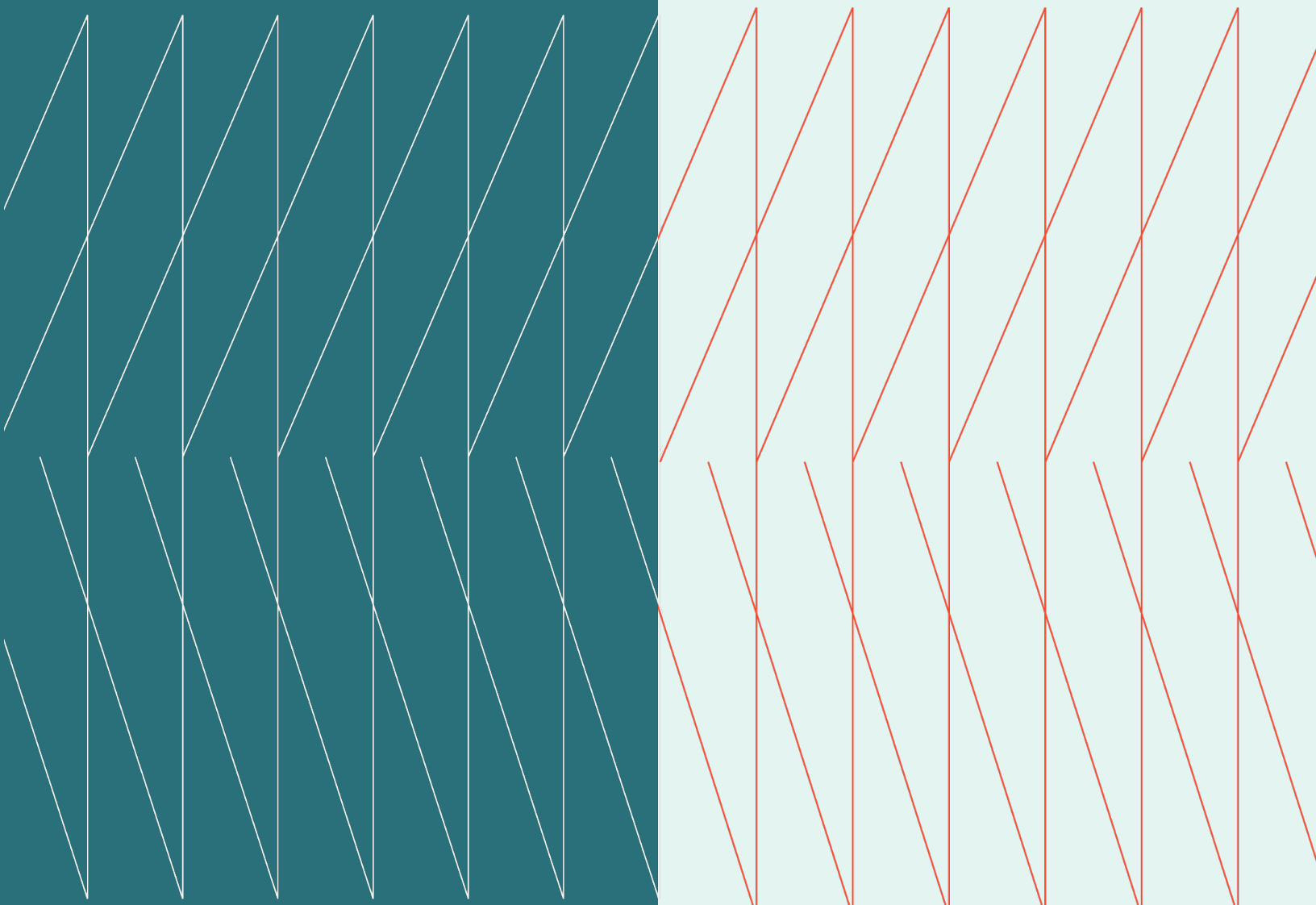
CISO

Expert Exchange

June 3, 2025

kyndryl

Executive Summary



Hosts:

Denis Villeneuve
Cybersecurity and Resilience Practice Leader, Kyndryl Canada

Tony De Bos
Vice President, Governance, Risk and Compliance, Kyndryl

Overview

In this CISO peer exchange, security leaders from various Canadian organizations discussed critical cybersecurity challenges. Participants shared insights on the security and resiliency implications of artificial intelligence. Key themes include managing data protection in the age of AI, addressing the third-party risk management challenges security posed by AI, mitigating the threat of AI-powered social engineering attacks like deepfakes, and navigating the future security challenges of autonomous AI agents.

Expert Exchange themes

- Data Protection Challenges with AI
- Securing AI Tools and Third-Party Risk
- AI Deepfakes and Social Engineering Attacks
- Agentic AI Concerns
- Responsible AI Use and Governance

Data Protection Challenges with AI

A core challenge for security leaders involves protecting organizational data when it interacts with AI solutions. Participants emphasized that while AI is often viewed as a new technology, the fundamental problems of data security and understanding where data flows and how it is used remain.

- Participants agreed that data is the first line of defense and that robust data management practices are essential. This includes understanding what data exists, where it resides, and how to classify and protect it, especially in light of privacy regulations.
- Securing data involves implementing traditional data loss prevention controls on endpoints, networks, and SaaS applications to ensure data remains within designated boundaries. One participant shared that their organization implemented stricter controls preventing access to e-mail and drives from non-company networks.
- While there was agreement that data is foundational, one participant highlighted that AI models present unique complexities compared to traditional data. They noted that the internal workings of models are often difficult to understand fully, introducing new vulnerabilities like prompt engineering risks that require additional security considerations beyond just data protection.
- Some organizations have blocked access to known external AI tools by way of technical controls. However, participants noted that employees often find creative ways to bypass these controls, such as moving data to personal accounts, making enforcement difficult and requiring continuous adaptation.

Securing AI Tools and Third-Party Risk

The proliferation of AI features embedded in various software products, and the reliance on third-party providers creates significant security challenges, particularly regarding the management of unsanctioned tools and potential data exposure. Participants acknowledged that AI is becoming a pervasive element in modern applications.

- Many organizations face the challenge of numerous unsanctioned AI tools being used internally by employees seeking productivity gains. One participant reported identifying hundreds of AI solutions in use, with only a small fraction officially approved.
- The rapid integration of AI into software-as-a-service products means organizations must evolve their procurement and risk assessment processes to account for embedded AI functionalities and potential data usage by vendors. Integrating risk assessments into the procurement process is a practical step organizations take to evaluate how potential AI solutions will handle and use data before they are adopted.

- A primary concern is ensuring third-party vendors handle organizational data responsibly when using AI in their environments. One member shared that they require vendors to work within the organization's controlled environment.

AI Deepfakes and Social Engineering Attacks

Participants are observing increased sophisticated attacks leveraging AI, particularly deepfakes and enhanced social engineering attempts. These attacks often aim to impersonate executives to trick employees into making unauthorized actions, such as transferring funds.

- Participants discussed that low-level employees, especially in finance and HR, are frequent targets for these attacks because they have access to systems that can yield financial returns for attackers, even though they may not perceive themselves as high-value targets.

- Organizations are implementing mitigation strategies such as establishing internal callback protocols to verify instructions. One participant suggested using internal codewords updated regularly so that only verified employees would know to confirm identity during suspicious calls.

- Beyond technology, organizational culture and established processes like bureaucracy can act as effective deterrents. One participant stressed the importance of avoiding a culture where employees feel pressured to immediately comply with urgent, unverified demands from perceived authority figures. Targeted training for high-risk departments like HR and finance is also crucial.

Agentic AI Concerns

A significant future concern raised by security leaders is the emergence of agentic AI, where autonomous agents can communicate and operate independently. This capability removes the human "in the loop" for specific interactions and introduces new security complexities that organizations are just beginning to understand.

- The ability of AI agents to communicate directly with other systems and agents creates a "grey area" where visibility and control over their interactions and data exchanges become challenging. Participants noted this is a significant evolution from previous system-to-system communication methods like application interfaces.

- A key challenge identified is the immaturity of security frameworks specifically designed for managing AI agents. Participants highlighted the need for robust identity and access management solutions that can effectively identify, authenticate, and authorize autonomous agents and manage their varying levels of categorization and permissions.

- Participants agreed that this area requires close monitoring and careful consideration, as the potential for autonomous agents to escalate risks without human oversight is significant. There was discussion about the limited understanding of how complex models behave autonomously and the potential for unexpected or undesirable outcomes.

Responsible AI Use and Governance

Effectively governing the use of AI involves balancing the drive for innovation and productivity with the need to manage associated security and privacy risks. Security leaders are tasked with establishing frameworks and educating stakeholders to ensure AI is used responsibly within the organization.

- Participants emphasized the need for a governance framework that prompts organizations to consider the security and ethical implications of AI use, including the potential for privacy violations arising from combining and analyzing data.

- Integrating questions about AI use into existing processes, such as procurement risk assessments, helps ensure that potential AI-related risks are identified and factored into decision-making. This demonstrates a commitment to responsible use.

- Awareness and education for employees are critical components of responsible AI adoption. This includes training on policies governing AI use and highlighting the risks associated with using unsanctioned external tools, reinforcing that employees should not input sensitive company data into third-party AI services.

- A key challenge involves educating business leaders and other stakeholders who may primarily focus on the productivity and cost benefits of AI. Security leaders must find ways to clearly communicate the "real risks" beyond just the benefits and demonstrate what those risks look like to gain buy-in for mitigation efforts.

Summary

CISOs are working to keep up with the rapid adoption and evolution of AI at their organizations. While there is pressure from employees and leaders to lean into the technology, CISOs need to push their organizations to understand the costs of the efficiency gains AI enables, both from a financial and risk management perspective.

To learn more about the Kyndryl Canada CISO Expert Exchange or to become a member of this community, please visit this website.

kyndryl