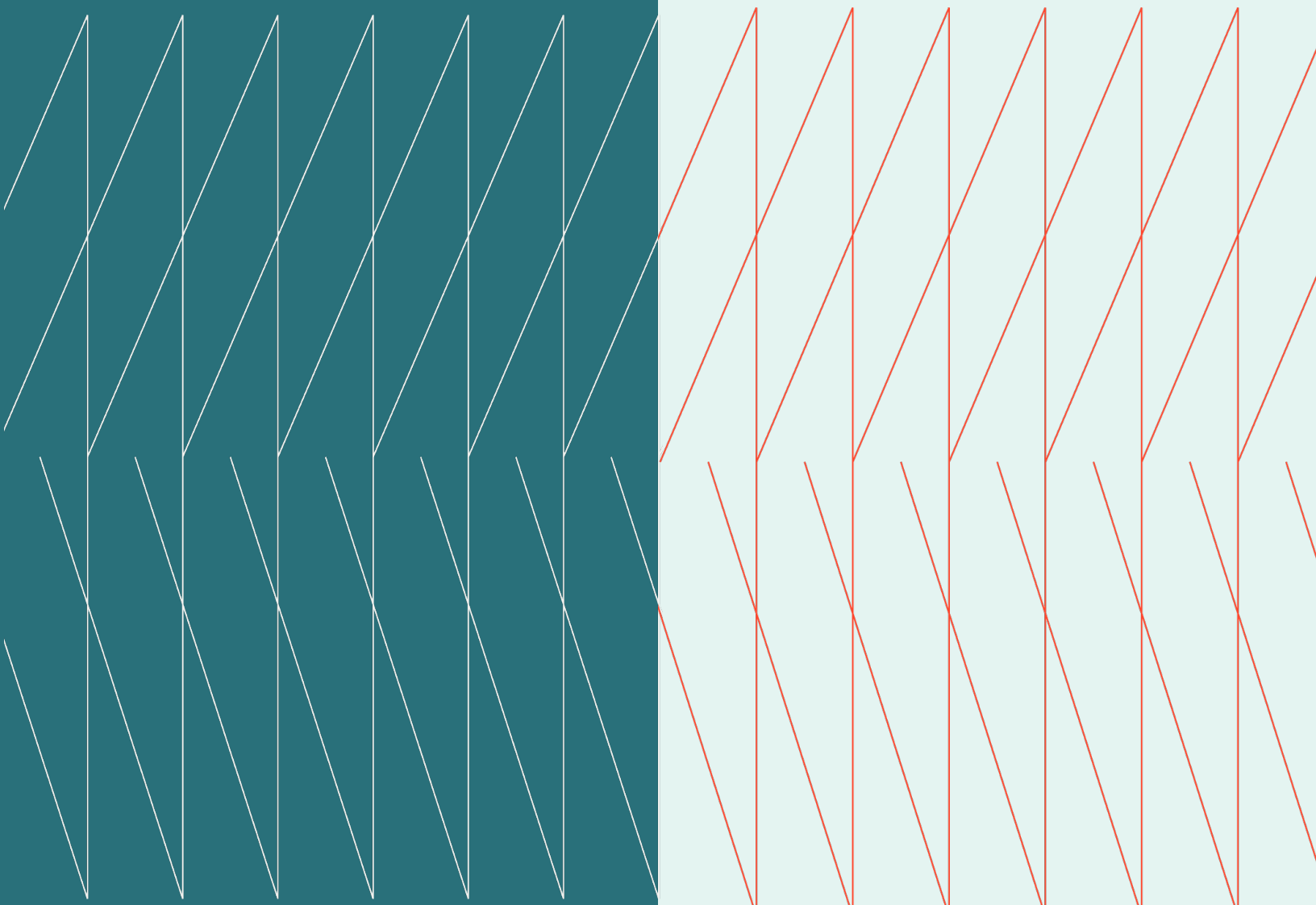
CIO/CTO

Expert Exchange

July 25, 2024

kyndryl

Executive Summary



Hosts:

Stewart Hyman
Chief Technology Officer, Kyndryl Canada

Adeel Saeed
Global CTO - Security and Resiliency, Kyndryl

Overview

In this Expert Exchange, CIOs and IT leaders from various industries discussed the opportunities and challenges of generative AI, cybersecurity and resiliency.

The exchange consisted of two main topics: generative AI use cases, how leaders determine the technology's value, and cybersecurity and resiliency in the age of generative AI. The participants shared their experiences, insights, and questions on how they are implementing, evaluating, and protecting generative AI solutions in their organizations. The exchange also explored the possibilities of collaboration and data sharing among peers and stakeholders to enhance cybersecurity and resiliency.

Expert exchange themes

- Generative AI Use Cases and Value
- Cybersecurity and Resiliency in the Age of Generative AI
- Collaboration on Cybersecurity

Generative AI Use Cases and Value

- The conversation began by focusing on generative AI's use cases and value. The participants discussed using generative AI to improve their domains' productivity, efficiency, customer experience, and innovation.
- They reviewed examples of generative AI applications in various fields, such as insurance, healthcare, software development, and education. They also discussed the benefits and challenges of measuring and communicating generative AI solutions' value and return on investment. Participants discussed how each LLM has their strengths and weaknesses for specific use cases.
- The group shared best practices for defining and aligning the metrics and outcomes of generative AI projects with the organization's business objectives and priorities and engaging the stakeholders, customers, and customers in the generative AI development and adoption process.
- Several group members need help with the expense of AI and are looking for low-cost solutions to pilot, building out capabilities and customized models from these initial pilots.
- "We use generative AI to simplify policy interpretation, automate decision-making, and provide personalized recommendations. This has increased customer satisfaction, reduced errors, and saved us time and money."

Cybersecurity and Resiliency in the Age of Generative AI

- The second topic of the exchange addressed the cybersecurity and resiliency implications of generative AI, both as a threat and an opportunity. AI poses new and complex cybersecurity threats, such as adversarial attacks, spoofing, and manipulation, that require advanced detection and mitigation strategies. Opportunities for using generative AI to combat threats were also discussed. Members brought up anomaly detection, threat intelligence, and incident response as use cases for enhancing organizations' security posture and resilience.
- Participants discussed how data protection is a critical and challenging aspect of AI. It involves complying with various regulations, such as GDPR and PIPEDA, and ensuring the consent, transparency, and accountability of data processing and sharing. Data protection also requires a holistic and proactive approach that covers the entire data lifecycle, from collection and storage to analysis and disposal. Participants discussed the tradeoffs between innovation and privacy and fostering a culture of responsibility among customers and providers.
- Best practices were shared for adopting a responsible AI framework that covers the principles, policies, and practices for generative AI use and governance. These include using data provenance and verification tools like blockchain, digital signatures, or certificates to track and authenticate the generative AI data and models.

Collaboration on Cybersecurity

- The final topic of the exchange explored the possibilities and benefits of collaboration and data sharing among peers and stakeholders to enhance cybersecurity and resiliency.

- The participants discussed how they are participating in or interested in participating in various forms of collaboration and data sharing, such as industry—or sector-specific forums, networks, or communities of practice, threat intelligence sharing platforms, networks, or communities, security research or innovation platforms, networks, or communities, and security standards or frameworks.

- They also discussed the challenges and best practices of collaboration and data sharing on cybersecurity. They shared best practices of defining clear and common goals, objectives, and expectations for the partnership and data-sharing activities and using designs designed to secure, reliable, and interoperable platforms, tools, or protocols for the collaboration and data-sharing activities.

- "We collaborate with other CIOs and IT leaders in our sector to share threat intelligence, best practices, and solutions. This has helped us improve our security posture, awareness, and use our peers' collective knowledge and experience."

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

kyndryl