CISO Cross-Industry

Expert Exchange

Q1 Executive summary
January 28, 2025

kyndryl

Overview

In this Expert Exchange session, several CISOs convened to discuss generative AI implementations, concerns around AI, and governance of internal AI use. The agenda was created based on advance interviews with participants.

Host

Jim Carrigan–Kyndryl – Global VP, Revenue Growth, GTM and Alliances Cyber Security and Resiliency Practice

Key topics

Generative AI is inevitable

- Regardless of industry, most companies are implementing generative AI, machine learning and automation in various ways. The group members shared a number of use cases they are piloting, with examples including improving manufacturing process quality and providing more expedited customer service.

- CISOs commonly use tools included with many "big box" technology solutions or, in some cases, create their LLMs to keep company data walled off from open-sourced generative AI tools. It is sometimes difficult to use big box tools because the company can't put its security settings in place. A member described how it seems like vendor solutions "are black boxes with intentionality,"so it's essential to monitor how a tool performs in the actual environment it needs to before fully committing to it.

- One CISO described their decision-making process regarding AI tools as having three decisions to make: what the tool does for the company's security from an offensive perspective, what it does for the company's security from a defensive implemented to reward positive cybersecurity behaviors and penalize risky actions, using incentives and disciplinary measures to promote a security-rich culture.

> “We had 486 generative AI projects around the business last year. Only 13 passed the assessment stage of the project to be funded and moved forward. Either the quality is not there, or you’re stepping all over privacy issues and it's not worth dealing with this."
>
> – CISO Expert Exchange Member

Generative AI implementation comes with concerns

- While generative AI can come with a lot of promise, it also involves a lot of challenges. Company executives and board members may be interested in exploring new use cases but lack an understanding of what AI use entails and the measurable value gained from implementation. (e.g., if even 20 percent of company operations were performed by generative AI, the power needed to run those data centers would be astronomical).

- Another concern is the ethics, liability, and security issues surrounding keeping humans in the decision-making loop. An executive explained that if you take humans out of the equation, then it's just one AI talking to another AI. It's up to the business to decide the threshold for AI involvement in decisions. In many cases, leaders find generative AI solutions unreliable for many business decisions that need to be made, highlighting the need for ongoing human involvement.

- Concerns around costs and security are prompting organizations to do thorough vetting of any use cases. Especially given the different understandings of what AI is, there are often better, simpler solutions than AI. In many instances, AI is not necessary for business.

"How, as security practitioners, are we putting controls in place? There are a million different models and hyper-specific ones. How do we assess those models' risk and drive towards more consistent use of vetted models?"

– CISO Expert Exchange Member.

Robust governance structures for the use of AI

- The CISOs discussed creating governance structures and guardrails to safeguard the use of generative AI by employees who may have a broad range of understanding and interest in the new tools. For companies that both serve other client companies (as technology consultants, for example) but also produce some of their products, it is essential to put policies in place for data sharing (or not) in LLMs.

- Many organizations are codifying formal acceptable use policies (AUPs) so that employees know how to use company data safely. A member pointed out that it is often easy to tell when lower-level employees or applicants to the company are using generative AI because the quality is so bad.

- One way leaders are introducing and beginning to work with the new technology is by creating walled-off, bespoke areas where their teams can safely work with their data. This has additional benefits beyond security. One member pointed out that using the company's data yields better results than using an open-source LLM.

- Another leader shared that, at the same time that companies are ramping up the use of generative AI, some security departments are "going back to the dark ages" as they are removing their data from the cloud and putting it in separate systems that don't talk to each other for safety and cyber security reasons.

·"We did an open sandbox for people to play with AI. We provide the tools and instances to enterprise applications, ChatGPT, and everything else, as well as a place where people can play, feel comfortable, and get used to it. And we've had hackathons with AI and stuff like that to get people going. Here's a place they can play and don't endanger the corporation."

– CISO Expert Exchange Member.

kyndryl

The CISO Expert Exchange is hosted by Kyndryl. Please contact Jim Carrigan, Jr. 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.