Cross Industry CISO

Expert Exchange

Q4 Executive summary

October 10, 2023

kyndryl™

Overview

In this Expert Exchange session, several CISOs convened to discuss the topic of generative AI security and risk mitigation. The focus of the discussion centered on managing generative AI risks, and responsible use of generative AI in the workplace. The agenda was created based on advance interviews with participants.

Hosts

Michael Restivo
Kyndryl, US Sales Vice President, Security and Resiliency

Jerry Lack
Kyndryl Director, US Alliance Business Development, Microsoft

Dean Pratt
Kyndryl Associate Director, Google Cloud Evangelist

Key Topics

Generative AI Adoption and Implementation

- Generative AI has numerous use cases and companies are exploring ways to implement the technology. Automation using generative AI is extremely powerful and will increase in capability, maturing over the next 5-10 years. As organizations grasp the potential impacts AI could have for them, the technology has been elevated to enterprise-grade where there are controls with data scientists and specialists working on implementing it on specific use cases within organizations.

- Companies are testing the enterprise solutions being offered by service providers in the market, with many leaders finding that, at this point, such tools augment workers rather than reduce staff or solve big problems. For example, ChatGPT has helped level out skills as junior analysts are able to quickly learn and do things that only senior analysts could do a year ago. At one CISO's organization, they are collaborating with Microsoft on generative AI technologies, particularly in developing the enterprise version of ChatGPT and Copilot.

- Many risks are associated with the use of generative AI, and as the technology evolves, companies should develop strategies to protect their business operations. For example, the tool can write code for people who have never written code and can resolve daily business operational issues using a generative AI engine. However, the code needs to be supported and troubleshot to determine the security risks associated with it. In addition, there are browser plugins, applications, and specific large language models being built, some of which are intentionally harmful.

"We do have a longer-term strategy where once we get the enterprise version of ChatGPT to the point where it is ready for prime time, we will probably start locking down all of the open-source versions and start funneling all of our corporate users into the enterprise version."

— CISO Expert Exchange member

Generative AI for Business

Learn more →

Generative AI in Education

- Universities are considering how to use generative AI tools in the classroom from a pedagogical perspective. Most of the institutions are still in their infancy as leaders try to figure out how generative AI can be used to enhance the interaction of students, teachers, and learning school models while protecting data such as administration, finance, and enrollment management.

- Some educational institutions have developed policies to roll out generative AI programs for learning purposes. In one example, a university has drafted a set of guidelines for the safe and secure use of generative AI in a teaching environment. There is awareness that anything put on the public version of ChatGPT is not safe, so some policies are stipulating that people do not use sensitive data to help in processes such as drafting a memo or building a slide deck.

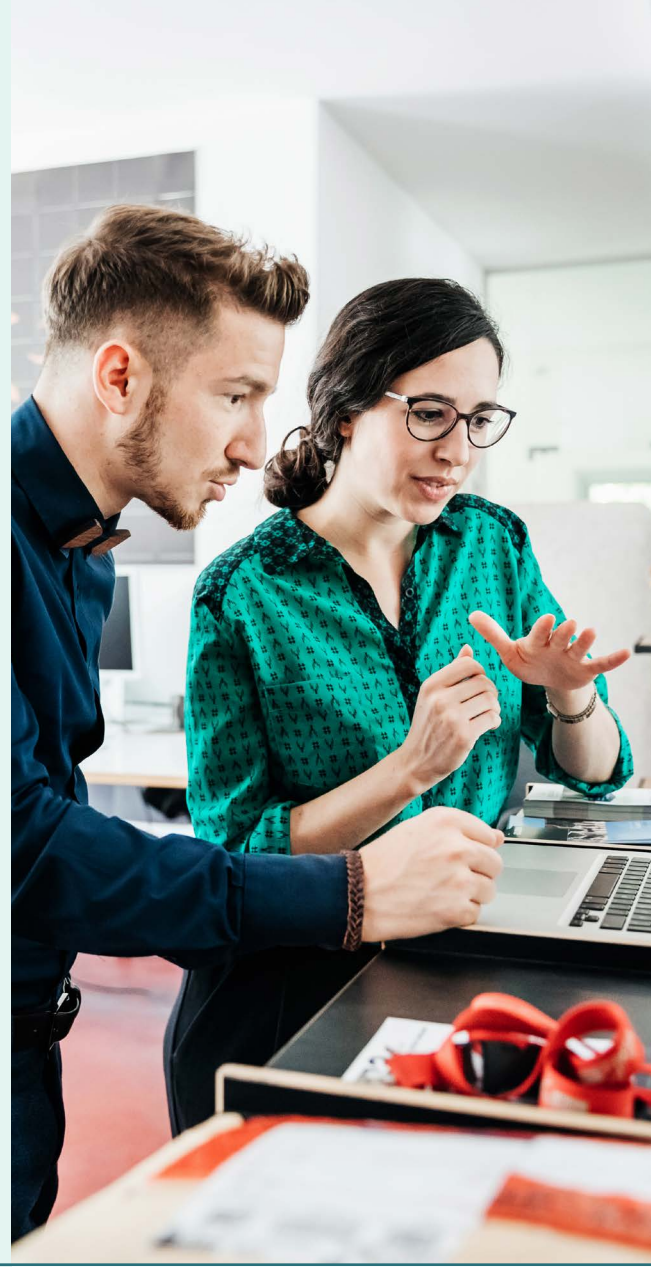
- Many universities are still reluctant around generative AI, but there will gradually be a shift as more students begin using ChatGPT. In one example, a university allows students to use ChatGPT to check their work for errors, but they are required to provide the screen print back to the professor.

"One of the first early caution cases was higher education, where people were putting their Ph.D. theses in the ChatGPT in order to get their boards or summaries or do spell-checking, not realizing that they were training the model with their educational research."

— CISO Expert Exchange member

Global AI-Driven Issues & Sustainability Concerns

Learn more →



Security Concerns and Responsible Use of Generative AI

- Safe and secure use of generative AI requires that businesses build guardrails for responsible adoption. In one example, a company is working closely with the CTO, compliance, and security departments over the whole AI program that is being implemented. The company has developed a policy and use cases are to be incorporated continually. Use cases and learnings continue to evolve while trying to discover risks associated with the new technology.

- A CISO mentioned how they developed a policy on the business side of generative AI early enough to stop people from posting sensitive data on the open source or public version of the technology. This is monitored using standard internet monitoring tools and there is pressure on the policy side to emphasize accountability to deter posting of sensitive data.

- One organization is using data loss prevention (DLP) policies to check for certain keywords with a centralized group that vets use cases and monitors what people are searching or entering. This provides greater visibility on how people are using the technology and triggering new ideas for use cases. In other cases, companies are working with vendors and Microsoft to ensure the use cases that are being considered are structured to protect company data. Another example involves a UI built on top of the open AI, internally hosted, to protect the data that enters the open-source AI.

"I think we all agree the use cases are absolutely endless and many have yet to be determined. One of the biggest challenges that we hear from customers and business leaders is how to put safeguards in place."

— Mike Restivo, Kyndryl US

"With generative AI being adopted at unprecedented rates, developing a clear strategy for identifying model efficacy and sensitive data exfiltration risks is paramount. As generative AI web and browser integrations become a more critical aspect of everyday workflow, a new emerging scope of security vectors demands proactive foresight and careful planning. Having a unified access approach, allowing for agile governance and response, is essential to a mature security posture that encourages responsible user adoption."

— Dean Pratt, Kyndryl US

kyndryl

The Expert Exchange is hosted by Kyndryl, Inc. Please contact Michael Restivo, Jerry Lack or Dean Pratt with any questions about Kyndryl or this Exchange.