



# 4 Ways to Make the Most of AI in Cybersecurity

Cybersecurity is always in flux. Some approaches that worked even a few weeks ago might be nearly obsolete today. One strategy that is taking hold, however, is the use of artificial intelligence (AI). Cybersecurity “is trending to AI just like it was trending to cloud maybe 10 years ago,” Sean Flowers, Executive Director at Ready Force Cyber, a cybersecurity workforce development company, said at a recent [GovLoop virtual event](#).

During the session, Flowers highlighted four ways that security teams make the most of AI. Khizar Sultan, Vice President of Workforce and Identity Governance and Administration Solutions at CyberArk, an identity security business, then looked at how agencies can modernize their identity-based security to integrate AI.

## Understand Risk Reporting

Because AI is in demand, enhancements are “slapped onto most of the security tools out there,” Flowers said. But “I think the strategy that would really help is getting a handle on risk reporting.” Understand your baseline risk and how AI tools can track and readjust that if risk rises or falls.

## Prioritize People, Process and Technology

A key to maximizing AI’s value is understanding where security is most needed. To do that, “look at your people, process and technology,” Flowers said. Here’s how that breaks down:

- **People:** People are usually the first line of defense — and the weakest, he said.
- **Processes:** Have a plan for responding to security incidents.
- **Technology:** Consider not just what you need now but also for the future, Flowers said.

## Cultivate a Cyber Culture

“Everybody is mandated to have a cybersecurity awareness program, which we find is a lot of check-the-box: I’m just going through this to satisfy the requirement,” he said. “What we really [need to] do is make it tailored towards the culture and the identity of the organization.”

Do that by tying training to the agency’s mission and using relevant processes and tools. Employees “will take a little bit more pride in protecting the information because now [they] know it’s just not some random scenario,” he said.

## Don’t Be Afraid

“Embrace AI,” Flowers said. “Don’t try to suppress it. There are too many tools out there and too many free capabilities for everybody to use it, and they will circumvent you if you try to put too many limits on it.” To minimize problems, educate and train employees on the latest threats and preventions. “Security is everybody’s responsibility,” he added.

# How to Get Your Identity-Based Security Up to Speed

WATCH THE VIDEO



Khizar Sultan

VP Workforce Identity Solutions, CyberArk

Many agencies are realizing that their legacy identity-based security solutions are beginning to age out. It shouldn't be a surprise. Identity solutions have played an essential role in cybersecurity for more than 20 years, with an evolving set of tools and tactics for identity and access management, privilege access management, governance and more. But the earlier generations were not designed to address the complexity of today's IT environment.

That's because security capabilities are just one aspect of an identity solution, said Khizar Sultan, Vice President of Workforce and IGA Solutions at CyberArk. As agencies increasingly rely on cloud- and software-as-a-service-based offerings, they need to address concerns around scalability and productivity, as well as the governance of artificial intelligence tools, such as AI agents. Legacy systems don't measure up.

In this [video interview](#), Sultan discusses how agencies can adopt an identity-first approach to cybersecurity. Topics include:

- The key attributes of an identity-first approach
- The connection between identity security and the user experience
- The importance of identity security to the use of AI solutions

*“Agencies are looking to adopt more modern identity solutions, especially because the demands of their organizations are increasing and they need more agility. And what users are expecting in terms of an experience is also rapidly moving forward.”*

— Khizar Sultan, CyberArk

## About CyberArk

CyberArk is a cybersecurity company specializing in privileged access management (PAM) and identity security solutions. Its primary focus is to help organizations protect privileged accounts, credentials, and sensitive data from cyber threats, insider attacks, and compliance risks. CyberArk is widely used by financial institutions, government agencies, healthcare organizations, and enterprises to secure their most sensitive data and systems.

[Learn more about CyberArk](#)

