



# 4 Ways to Shift to People-Centric Security

**Good cybersecurity has two basic components: the technology itself and the people and processes that put it into practice.** Unfortunately, many cybersecurity programs focus on technical problems and lose sight of the human element, said Ralph Hogaboom, Chief Information Security Officer at Washington’s Department of Natural Resources (DNR).

For example, many agencies build programs around standard frameworks, such as the National Institute of Standards and Technology’s SP 800-53, which specifies security and privacy controls. What most agencies lack, Hogaboom said, is a framework that centers on people.

“The valuable thing is where the people are,” he said. “It’s the people who are engaging with the data. It’s the people who get hurt when there’s a breach or when there’s system downtime that causes organizational outages or problems.”

At a recent [GovLoop virtual event](#), Hogaboom discussed how agencies can be more people-centric. Here are highlights from that discussion. As part of that event, CyberArk highlighted the evolution of identity-based solutions.

## Emphasize Processes Over Purchases

Good tools are important, but good supporting processes are crucial, Hogaboom said.

For instance, a solution for identifying vulnerabilities is effective only if the IT team follows through with remediation, he said. “There needs to be this hum of daily work where, as you’re seeing things, you start triggering that process,” Hogaboom said.

Even a technical process such as remediation can require a human touch, because the IT team often needs to coordinate with the people who “own” those systems. The process goes more smoothly when IT builds goodwill with those users.

“You can have a great cybersecurity tool that costs a lot of money, but if your people don’t know how to deliver real business outcomes from those tools, then you’ve just wasted your money,” Hogaboom said.

## Frame Risk in Terms of Outcomes

In theory, risk can be a useful lens through which to prioritize cybersecurity requirements. In practice, however, risk assessments are often too vague or miss the point completely.

Hogaboom cited a story that Jack Jones, creator of the Factor Analysis of Information Risk framework, frequently tells: When asked about the risk of a bald tire, most people respond that

the car could spin off the road, sustaining major damage and possibly injuring the driver and any passengers. But, Jones points out, he never mentioned a car — the tire could just as easily be hanging from a tree as a swing.

To be meaningful, risk assessments must be specific to a given context and mission. Think about firefighters using laptops to track the movement of fires. What is the risk of sharing files via USB drives? If the drives aren't properly secured, they could introduce a virus. But in practical terms, the real risk isn't the virus itself, said Hogaboom. It's the potential disruption to operations, which could endanger firefighters.

“And that's what I mean when I say I think one of those pitfalls [of risk assessments] is really zeroing in on the technology and forgetting that there are people out there,” he said.

## Make **Training** More Meaningful

Security awareness training has gotten predictable. A session on phishing, for example, might define the types of phishing, explain how to identify phishing attempts and recommend next steps. That's all good information, but it doesn't always hit home.

Hogaboom conducts what he calls quarterly security awareness “road shows,” in which he gives presentations to various state business units. While covering the basics, he tries to make the issues feel more real and more urgent.

In the case of phishing, that might mean talking about the market for credentials in the criminal supply chain. He might point out how a File Transfer Protocol credential for NASA.gov sells for about \$65,000 in Bitcoin right now, and then ask, “So, how much would your WA.gov credentials fetch for someone where the U.S. dollar goes a lot further?”

Hogaboom said the road shows are a lot of work, but he thinks they are worth it because they get people engaged in the topic. “I don't know anybody who's excited to see a pre-recorded security training,” he said.

## Cultivate Your **Cyber Talent**

Agencies are likely to find that their pool of cyber talent is growing, thanks to shifts in the broader job market. Hogaboom, for example, recently received several hundred quality applications for a cybersecurity analyst position. He said a tremendous amount of talent is available — if agencies can take advantage of it.

But finding the right talent is just the starting point. The real magic happens when those individuals coalesce in cross-functional teams, Hogaboom said. Agencies can cultivate those team dynamics even if employees are working in remote or hybrid office environments.

For example, DNR's cybersecurity team spends about 90 minutes each day on a team call, working through various issues together, such as reviewing out-of-state travel requests or dashboard logs and alerts.

The team also has a monthly “Consolidation Day,” when no normal business meetings take place to give staff time to work together on whatever projects they want — “like an R&D day,” he said.

When team members collaborate in these ways, “there are so many small moments of mentoring that happen and encouragement for each other,” Hogaboom said. “When they come to work excited and energized because it's filled with people they trust and want to spend time with, they're going to do a better job.”

*To hear more tips, watch the full event on demand.*



# 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](#)

