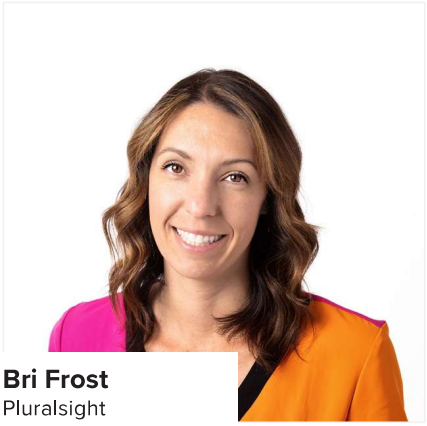
PLURALSIGHT

Future-proofing the security workforce

Continuous, targeted training and upskilling are as vital as technology in the fight against cyber adversaries



Bri Frost
Pluralsight

"PEOPLE ARE MORE WILLING TO LEARN AND MORE LIKELY TO RETAIN NEW INFORMATION WHEN IT'S RELEVANT TO THEIR DAY-TO-DAY ACTIVITIES."

Agencies face a multitude of challenges in building multifaceted IT teams that can respond to today's cyberthreats. The problems begin with the fact that there are not universally agreed-upon roles and responsibilities, so IT teams and security teams have to define those for themselves. The result is fragmented skill sets and siloed mindsets that focus on only traditional IT responsibilities or only security responsibilities.

IT employees often excel in operations but may lack cross-disciplinary expertise in areas such as cybersecurity, cloud and artificial intelligence, which are needed to address today's complex threats. Adversaries are leveraging AI, automation and advanced techniques to change the threat landscape, and they are outpacing the defensive capabilities and tools of static, siloed teams.

In addition, although vendors are quick to update their technology solutions to address new challenges, the government's budget and procurement processes typically don't allow agencies to buy the latest technology. Outdated infrastructure and slow-to-adapt strategies make it difficult for IT teams to integrate modern security and AI solutions fast enough to stay ahead of attackers.

Mapping skills to mission needs

It is possible for agencies to take a more strategic approach to skill development and create IT teams that deliver on the government's goals for cybersecurity. Such an approach requires moving beyond reactive, ad-hoc training and toward a skills-first workforce model. This includes role-based upskilling and scenario-based training. Relevancy and efficiency are the main goals. People are more willing to learn and more likely to retain new information when it's relevant to their day-to-day activities and when they can see the impact and benefit.

Agencies should aim to keep training plans specific by mapping skills to mission needs and providing learning paths that are targeted and role-specific—for example, cloud security engineers and AI-focused data analysts. In addition, training should include the practical, hands-on experience of real-world exercises so teams will be prepared when actual events happen. For AI specifically, employees should be able to experiment with the newest tools. Threat actors have already integrated AI into their attack campaigns, and it's essential for government agencies to get ahead of those threats.

The most important objective for skill development is implementing a

continuous learning culture from the top level down. Leaders should encourage learning and set an example by engaging in training themselves. They can help establish an environment where upskilling is ongoing, measured and tied directly to mission readiness.

Learn by doing in simulated real-world scenarios

Pluralsight's solutions provide the structure and insight agencies need to build strong security teams. We deliver fast, efficient training paths that enable agencies to close skills gaps and future-proof their workforce. Our role- and skill-based paths are mapped to multiple government guidelines, including the Defense Department Cyber Workforce Framework. DCWF describes the work performed by all elements of DOD's cybersecurity workforce.

For all our agency customers, we curate and tailor training to develop skills in IT, cybersecurity, cloud and AI so teams gain mission-critical capabilities quickly. Our high-impact courses teach those teams how to defend against real-world cyberthreats by understanding the techniques that attackers use.

For the practical application component, Pluralsight offers hands-on experiences in sandboxes, isolated lab environments and cyber ranges that accurately replicate the complexity of IT networks to enable practitioners to learn by doing in simulated real-world scenarios.

With Pluralsight's constantly updated content, IT teams can cross-train on all the necessary skills to keep up with evolving technologies and stay ahead of emerging cyberthreats. ■

Bri Frost *is director of security and IT ops curriculum at Pluralsight.*

ADOBE STOCK// VLADIMIR