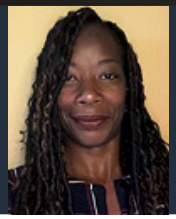
Closing the cybersecurity skills gap in government



State and local governments must do more to recruit cyber defense talent. Increasing diversity efforts, repurposing existing resources, and expanding outreach to academic institutions can be effective strategies. In this Q&A, **Maria Thompson**, former chief risk officer for the state of North Carolina and current executive government advisor for state and local government at Amazon Web Services (AWS), discusses how leaders can build a robust cybersecurity workforce for the future.

How challenging is the cybersecurity skills gap?

There's a definite shortage of individuals to monitor and maintain networks, which bad actors are targeting. When I was a state chief information security officer, for instance, we saw over 20 ransomware events in our state and local governments in one year. We analyzed the logs from security tools such as endpoint detection and firewalls. Generally, we identified that even though the organizations had security tools in place, the agencies didn't have resources to monitor and triage, or the right personnel or skillsets to identify, detect, and respond to anomalies in a timely manner and mitigate the blast radius of the event. This helped ransomware take hold.

How can agencies address this shortage?

First, you have to understand your organization's limitations and capacity. Agencies should conduct a gap analysis. They can then prioritize improvement that supports initiatives like incident response, data sensitivity, privacy, and data resilience.

They should also leverage vendor partnerships. There are security consulting and integration partners that can augment staff to support specific initiatives. As your internal teams build their skills, you can ramp down those vendor contributions.

How can leaders create a better talent pipeline?

Many states are focusing on building partnerships with academic institutions for internship, apprenticeship, and training opportunities. Organizations should also look at ways to modify their recruiting practices. Governments tend to be rigid in the requirements they're looking for. Agencies should instead look for potential team members with a broader spectrum of skills or experience.

Organizations can also create a mechanism for cybersecurity reskilling. For instance, AWS Academy has a program called AWS re/Start that creates training opportunities for unemployed and underemployed individuals to work in cybersecurity. This program accomplishes two main objectives: providing a pathway to employment and future-proofing the workforce by preparing them for jobs in a highly sought-after market.

What are some unexpected sources of cybersecurity talent?

Because I'm a veteran, I see a huge opportunity to recruit those who are either retiring or transitioning from the military. In North Carolina, we created an apprenticeship program for veterans to build and expand the cyber pipeline. We identified the veteran community as an untapped resource. North Carolina has the fifth-largest military population, so this was and is an opportunity to reskill and re-employ service members to public service.

How else can technology ease the cyber talent crunch?

Cloud services are top of mind because capabilities like automation can seamlessly integrate into operations. There's also artificial intelligence (AI). Security environments get inundated with security log data — a human can't parse all of it. AI takes the load off the generally overworked security teams, letting them really focus on those particular incidents in their environment that could cause some level of disruption.

AWS offers integrated and automated services like AWS CloudTrail, AWS Config, Amazon GuardDuty, AWS SecurityHub, and other security tools that supports continuous monitoring and identification of threats, and configurable ways to automate a response. These capabilities remove the tedious tasks for a small team and also ensure a consistent and timely response to threats.