SANS | GIAC CERTIFICATIONS

Beyond the Cybersecurity Talent Shortage Myth

Cisco's Approach to Hiring and Job Standardization

Helen Patton
Cybersecurity Leader at Cisco

Helen Patton, a cybersecurity leader at Cisco, says there is no cybersecurity talent shortage—we just need to learn to understand and identify the needed skill sets for specific roles. That calls for a more nuanced approach to discussing cybersecurity employment, emphasizing the need to look beyond traditional hiring practices and standardized roles to address the field's complex realities.

Patton challenges the widely held belief of a cybersecurity talent shortage. "My personal perspective is that we don't actually have a talent shortage in cybersecurity," she asserts. Instead, Patton argues that the real issue lies in "understanding the skill sets that are needed for the kinds of roles you have" and "finding the people who have those skill sets." She is particularly critical of the often-cited figure of 500,000 open cybersecurity positions. "I think it does everyone a disservice to talk about those numbers."

Instead, she argues that there should be a more nuanced discussion, pointing out that talent availability varies significantly by location. "Also, the numbers may not accurately reflect actual hiring intentions. As a CISO in my previous role at Cisco, I needed three times as many people as I had, but I couldn't hire them. So, is that gap the people you really need or the number you are actually hiring?" According to Patton, this highlights the discrepancy between perceived needs and actual hiring practices, suggesting that the true state of cybersecurity employment is more complex than often portrayed.

More Structured Definitions of Cybersecurity Roles

The perceived talent shortage is closely tied to the cybersecurity industry's lack of standardized job families, says Patton. "The industry isn't codified in what is needed regarding skills or jobs." This ambiguity contributes to the difficulty in accurately assessing workforce needs and finding suitable candidates. Patton notes that while efforts like the NICE framework exist, they are limited: "The NICE framework is a great starting point, but it's written by people who work in the government. It's not written by all the other verticals out there."

To address this issue, Patton predicts a shift towards more structured definitions of cybersecurity roles driven by regulations. "Because of regulations, I think we're going to see more structure put around what cybersecurity is and isn't." However, she cautions that this standardization may create new challenges. "You're going to have a square peg round hole kind of problem, like a mismatch between what an individual organization needs and what the industry says this role is." As a potential solution, Patton suggests moving away from traditional job levels and towards an apprenticeship model. This approach, she believes, would better accommodate local contexts and rapid technological changes.

The CISO Role Will Split and Change

Patton foresees a significant evolution in the CISO role and overall structure of cybersecurity teams. "The role of the CISO is being defined and hasn't been defined until now." This lack of clear definition has led to ambiguity in the scope and responsibilities of the role. Patton traces this ambiguity back to the field's historical development: "If I go back 20 years, the CISO was responsible for information security, not cybersecurity." However, the rise of the cybersecurity industry has shifted focus towards "defense against external attacks," which Patton notes is "a subset of information security, but it's not all of information security."

This evolution has created tension in the CISO role. She observes that enterprise security tends to lean more towards comprehensive information security in larger organizations, while medium and small companies focus primarily on protecting against cyber-attacks. Given this divergence, Patton predicts a split in responsibilities: "I think the GRC function will go more towards enterprise security and information security, and then the CISO function will be cybersecurity, technology controls, monitoring, and detection and response." This separation would allow for more specialized focus in each area, with GRC handling broader information security concerns while the CISO role concentrates on technical cybersecurity measures.

Search for Internal Talent

Patton's analysis reveals the complex nature of the cybersecurity workforce landscape. Her call for nuanced understanding, redefined roles, and innovative approaches to talent acquisition and development offer a fresh perspective on addressing the industry's challenges. As the field evolves, organizations may need to rethink their approach to cybersecurity roles and team structures. Patton's final advice resonates strongly: "When hiring, look internally first; look at business analysts, project managers, financial analysts, teachers, and HR people." In the end, Patton reminds us, "The talent shortage is a nuanced problem, and hence, we need to talk about it in a more nuanced way." This thoughtful approach may well be the key to navigating the future of cybersecurity workforce development.

> "My personal perspective is that we don't actually have a talent shortage in cybersecurity."