Successful Strategies for Cybersecurity Hiring: for Human Resources and hiring professionals

The shortage of cybersecurity talent can make it challenging for organizations and Human Resource departments to hire and retain a skilled cybersecurity workforce. Additionally, organizations need to build a human capital pipeline that brings new candidates into the field, and increases representation from under-represented populations. Adoption of one or more of the following strategic concepts may allow a hiring manager to reduce time-to-hire, identify gaps in their cybersecurity workforce, develop career pathways and diversify their teams. Resources for a deeper understanding of these ideas may be found on the reverse of this document.

Assess the Current Cybersecurity Environment

Every individual has a work role in organizational cybersecurity. Organizations can use the NICE guidebook , Cybersecurity is Everyone's Job to identify work roles by business function, defining each role and function as a part of the cybersecurity workforce.

Use Knowledge, Skills and Abilities tools, like the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, the Department of Labor's O*Net tool and the Cyberseek.org website to evaluate workforce needs. This may help to improve the overall understanding of cybersecurity work in an organization.

Create a demographic profile of the cybersecurity workforce and determine if staffing is designed to support diversity objectives. Assess the time it takes to hire new personnel (time-to-hire) and annual retention rates. Evaluate salaries, using tools like the Department of Labor BLS Wage data by Area and Occupation, against competitive data for the local job market and national averages.

Review Job Requirements

Using the NICE Framework, describe the necessary Tasks, and related Knowledge, Skills and Abilities to build job descriptions aligned to business needs. Organizations are re- evaluating requirements such as college degrees, advanced certifications and experience requirements that might unnecessarily discourage otherwise qualified talent from applying or being considered. The U.S. Bureau of Labor Statistics uses a system to assign categories for entry-level education, work experience in a related occupation, and typical on-the-job training to each occupation.

Standardize Cybersecurity Job Titles

Cyber Threat Hunter? Information Security Analyst? Job titles are different across industry, academia, and government. The NICE Cybersecurity Workforce Framework and the Department of Labor's O*Net tool can help provide some examples; review the Cyberseek website to see other common titles in use.

Remove Hidden Bias in Position Descriptions and Hiring

Seek to remove language from job advertising and position descriptions that may discourage diverse candidates from applying for open positions, i.e. the use of masculine gendered nouns or references to military-style approaches. This can be difficult to recognize without guidance from experts or the use of text-based tools that both spot biased or coded terminology and offer suggestions to use in their place.

SHRM.org identifies masking strategies and blind interview steps to strip identifying information from resumes and job applications before sharing with the hiring teams. Invite a diverse team from across your organization to assist in panel-style reviews of candidates.

Be Candidate Centric in Hiring

Make the application process a candidate-centric experience. Consider posting information on your Career portion of the organization website that describes the steps in the hiring process, what interactions the candidate may expect to have, examples of interview questions per department or position. Ask for and include anonymized candidate feedback.

Screen for Talent with Aptitude or Skill Assessment Tools

Critical Thinking

Critical Thinking Asking Who, What, When, Where, Why and How questions, at the appropriate level can help candidates show analytical, interpretation, evaluation, problem solving and communication skills.

Interviewing CyberSecurity candidates

Finding the right candidate for cybersecurity positions can be a challenge. HR managers and IT professionals can work together to balance performance- based questions with education, skills and organizational culture assessments.

Verbal and Written communication skills assessment: Re-evaluate the importance of soft skills in cybersecurity positions. Interviews should allow candidates to display soft skills as well as hard skills.

Ex question: Can you give an example of how you explained a technical problem to a non-technical person?

Unicorns are rare – don't build job descriptions and interviews based on all or nothing criteria. Guidelines like the Aspen CyberSecurity Groups Principles for Growing and Sustaining the Nation's Cybersecurity Workforce, offer insights and guidelines to help build organizational pipelines for the cybersecurity workforce.