Executive Summary: Critical Challenges Facing the Nation's Cybersecurity Workforce

The Cybersecurity and Infrastructure Security Agency (CISA) sponsored research by Carnegie Mellon University (CMU) Software Engineering Institute (SEI) to explore critical challenges facing the nation's cybersecurity workforce shortage. These studies explored the top in-demand cybersecurity roles, career progression, and talent identification and assessment.

Universally, the studies emphasized the need for a standard framework from which to define and describe cybersecurity work. The studies suggest that the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework should provide a common lexicon for describing cybersecurity workforce requirements, for employers, educators, hiring managers and others.

Identifying the skills gap: *Cybersecurity Careers of the Future Report*

Findings exposed great variations in the way organizations title and describe job positions. The lack of uniformity and coordination across the way we talk about cybersecurity positions makes closing the workforce gap more difficult. CMU-SEI deconstructed cybersecurity job positions down to the knowledge, skills, and abilities (KSAs) that make up each role. CMU-SEI aligned the KSAs to NICE Cybersecurity Workforce Framework Work Roles to analyze the top in-demand cybersecurity Work Roles.

Top 5 In-demand cybersecurity Work Roles

1. **Information Systems Security Developer**
2. **Information Systems Security Manager**
3. **Systems Developer**
4. **Research & Development Specialist**
5. **Software Developer**

The following Work Roles are important entry-level positions to advance towards the top 5 in-demand positons:

- System Administrator
- Network Operations
- Specialist Cyber Operator

As more threats emerge and technology changes, organizations will likely need employees with more experience in Vulnerability Assessment Analysis and Security Control Assessments.

Finding the Right Fit: *Cybersecurity Talent Identification and Assessment Report*

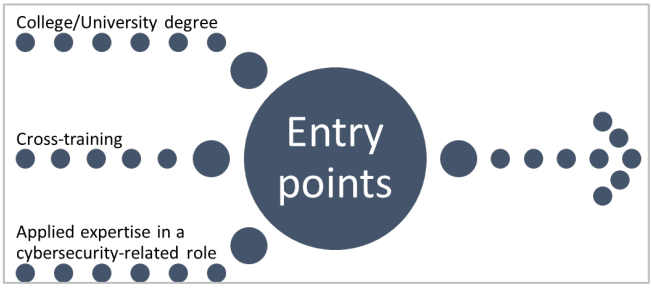
Findings highlight the difficulty in designing a one-size-fits all assessment tool to identify individual skills and capabilities. The report explores how cybersecurity talent is currently identified and highlights assessment capabilities that could be leveraged to find ideal applicants for vacant positions.

- In addition to the high number of cybersecurity job vacancies, many employers feel their current cybersecurity teams are not properly trained to combat the latest security threats.
- Though generalized aptitude tests are a useful tool in evaluating fit, the combination of additional assessments that evaluate potential success are likely to better identify talent.
- Candidates with great potential might not pass a key word screening on a resume search. This issue is made more troubling due to the lack of standard lexicon or use of a common cybersecurity framework.
- Early education and skill training is key to developing strong competencies—cyber ranges and competitions can be a useful training ground turned recruiting tool.

Advancing the team: *Cybersecurity Career Paths and Progression Report*

Findings highlight the uniqueness of the cybersecurity career path—one that can favor proficiency in skills and problem solving, and technical aptitude, over a traditional higher education and credentialing route. In other words, there are many ways into the field also making it more complex to navigate.

- A foundational start to a cybersecurity career includes some combination of a technical groundwork, an IT-related education, an industry credential, and/or applicable work experience.
- Applying for positions often requires some level of higher education to demonstrate an aptitude to succeed in that position. That said, those with extensive experience may also succeed in technical Work Roles.
- Though academic degree programs make up the largest entry point into cybersecurity, cross-training from current IT roles, and applied experience from other technology-related fields are also successful pathways into cybersecurity.
- In addition to cybersecurity-related work experience, investing in more specialized training and certifications are success factors for progression in this field. With the rapidly changing nature of the domain, career pathways and required training must be reviewed and updated regularly.
- Cybersecurity associations, working groups, and conferences provide an excellent opportunity for professionals to enhance both their personal and professional development.



Links

To read these reports in full, visit the National Initiative for Cybersecurity Career and Studies (NICCS) Cybersecurity Resources.