

[«The Collaborative Alliance to Develop New Cybersecurity Council and Professional Recognition as part of the UK's National Cybersecurity Strategy](#) | [Main](#) | [CCSP and CCSK: Which Cloud Security Credential Is Right For You?](#) »

27 August 2019

IT PROFESSIONALS: USE THE SECURITY SKILLS SHORTAGE TO YOUR ADVANTAGE



A cybersecurity skills shortage is expected to result in [3.5 million](#) unfilled positions by 2021. Research [from ESG](#) finds 51% of organizations believe they have a “problematic shortage” of cybersecurity skills – an increase of 7% year-over-year.

Clearly, the skills gap is a serious problem, impacting an organization’s ability to keep up with software vulnerabilities, harden devices, respond to security issues quickly and strategically manage security in an ever-evolving threat landscape. With the odds stacked against

them, businesses must find new ways to recruit and retain skilled security employees and proactively address the lack of talent to fill critical roles.

Here’s what IT and potential security professionals should know about tackling this major skills shortage – and strengthening career prospects.

Organizations must get creative with hiring

A shortfall of talent with traditional experience and education in security is only expected to intensify, so employers must consider hiring talent with less typical work histories to take on security roles.

Still, many hiring managers think it is necessary to look for candidates with traditional technology credentials — college degrees in tech fields, for example. But this is a mistake when it comes to hiring during a talent crunch. Businesses today should open themselves up to applicants whose nontraditional backgrounds bring value to the table. When positioning yourself for a security role, make it known how your previous experience, education and soft skills equip you with new ideas to meet the challenges of improving cybersecurity.

Security leaders and hiring managers will need convincing to recast their expectations and look to candidates with a wide range of competencies. But employees who see these jobs as an opportunity to use existing skills, develop new skills and shift gears in their career are viable candidates more likely to commit to a company for the long term.

Developing employees internally

An existing internal talent pool is an excellent resource for cybersecurity roles. If you’re coming from general IT, engineering, compliance, networking and other disciplines with technical knowledge and a natural curiosity, you could very well be the right candidate for taking on a new career challenge.

Security is increasingly a shared responsibility across all lines of business, and a solid, in-house training program helps identify employees with the aptitude for security. As an existing employee seeking a new security-focused role, consider job rotation programs and job shadowing across departments as a viable first step.

Businesses also look for training and certification programs to help transitioning internal candidates gain valuable security education to enhance the skills they bring to the job. But there’s no reason to wait. It will be highly advantageous for you to get a step ahead and move forward with [professional development](#) and [certification](#) on your own.

Tapping outside resources

Forward-thinking employers are also tapping local technical, community and traditional colleges to find students who have cybersecurity skills or are looking for a career in cybersecurity. Be sure to leverage [resources available](#) in your community.

SEARCH

(ISC)² LINKS

[\(ISC\)² Home Page](#)

[\(ISC\)² Members Site](#)

Follow (ISC)² on Twitter 

CATEGORIES

[\(ISC\)² Chapters](#)

[\(ISC\)² Events](#)

[Center for Cyber Safety and Education](#)

[Cloud Security](#)

[Cybersecurity Certifications](#)

[Cybersecurity Training](#)

[Cybersecurity Workforce](#)

[Digital Forensics](#)

[Ethics](#)

[Government](#)

[Insider Risk](#)

[IT Security](#)

[Legal](#)

[Malware](#)

[Network Security](#)

[Operations Security](#)

[Privacy](#)

[Ransomware](#)

[Risk](#)

[Software Development](#)

[Spotlight](#)

Another smart move is developing relationships with [associations](#) that offer membership and certification for security professionals. As organizations actively seek out a pipeline to security talent, you have much to gain through these avenues.

Waiting for qualified candidates to come to them is not an option for employers in this job market. A proactive and collaborative approach between employee and employer is essential for fostering talent in the industry and successfully addressing the cybersecurity talent gap. With the right strategy, you have the power to help fill the gap and achieve more in your career.

Want to take advantage of the security skill shortage? Learn how in the [Add Security to Your Skill Set \(and How to Do It\) eBook](#).

 Posted by [ISC2 Management](#) on 27 August 2019 at 08:30 AM in [Cybersecurity Certifications](#), [Cybersecurity Workforce](#), [IT Security](#) | [Permalink](#)

 Tweet

 Like 11

Comments

Comment below or sign in with  Typepad  Facebook  Twitter and [more...](#)

(URLs automatically linked.)

Email address is not displayed with comment.

POWERED BY  TypePad