Bridging the widening cybersecurity skills gap





In today’s cyber landscape, the challenges loom large. Evolving threats and technologies have reshaped the battleground, making traditional on-premises infrastructure

defenses obsolete. Despite advancements in security tools, a pressing issue remains: a significant shortage of skilled professionals.

In addition to the compromise of mission-critical systems and networks, enterprises grapple with reputational damage, financial losses, compliance hurdles and legal ramifications from a cyberattack. Organizations must not only address current risks but also anticipate future threats, safeguard sensitive data, comply with regulations, meet industry expectations and prioritize customer satisfaction. These imperatives underscore the critical need for businesses to bridge the cybersecurity skills gap, ensuring the continuity of digital transformation that drives competitiveness and resilience in the face of these evolving threats.

Where the industry is at with the issue

In its annual Cybersecurity Workforce Study released last October, ISC2 found that the gap between the number of cybersecurity professionals available and needed increased by 12.6% over the previous year even though the cybersecurity workforce as a whole grew by 8.7%. ISC2's findings show that a large percentage of respondents believe they do not have enough cybersecurity professionals in their organization to prevent and troubleshoot cybersecurity issues. Across industries, 67% of cybersecurity professionals reported that their team is understaffed.

Technical expertise is essential, but other skills are equally vital

As our understanding of security has matured, the demands associated with cybersecurity positions have grown. Although technical proficiency remains crucially important, it is no longer sufficient on its own. Yes, some employees may understandably gravitate to a particular aspect of security

such as threat analysis or incident response. And supporting a niche role is entirely possible and valued in many organizations. However, to be effective in a general practitioner or leadership role requires today's cybersecurity professionals to possess a multi-faceted skill set. Beyond technical skills, professionals in these roles must also grasp intricate industry regulations, risk management, organizational processes, security prioritization and customer expectations as well as adapt to continuous learning and thrive in high-stress environments.

Bridging the gap – how do organizations develop, attract and retain such professionals?

Fortunately, there are many proven strategies enterprises can embrace, and steps they can take, to address the cybersecurity skills gap – a gap that will only widen as organizations realize that the demand for professionals who possess such competencies will continue to outpace their availability for years to come.

Executive, IT and cybersecurity leaders can and must take action to address this reality. Fundamental, required actions include:

- Revisit the organization's environment and culture: It is crucial for both leaders and the entire enterprise to acknowledge that cybersecurity, though closely tied to IT, is a complex discipline. This field demands not just dedicated resources but also a unique reward system and organizational structure. These elements should be in alignment with the crucial role cybersecurity plays in protecting an organization's assets, reputation and its ability to conduct business. Just as importantly, this necessitates not only the recruitment of individuals who possess the aforementioned multifaceted skill set, but

also the proactive development of such talent.

- Prioritize the work-life balance and job satisfaction of employees in cybersecurity roles: Unfortunately, in many companies, cybersecurity roles are only valued when a breach occurs. Leaders must take steps to support the mental and physical health of cybersecurity professionals who often feel they are “on call” at all times. This includes recognizing the demanding nature of their roles and the importance of maintaining resilience and job satisfaction.
- Invest in comprehensive professional development: Continuous training is critical to maintaining relevance in the field of cybersecurity. Organizations should provide opportunities for their cybersecurity employees to enhance their skills and stay abreast of emerging threats and technologies. This includes employer funded technical training and additional opportunities for development in areas such as compliance, risk management and leadership – not to mention evolving areas like AI. It is also critical to support participation in industry conferences and professional associations. These perks demonstrate a commitment to ongoing learning and help retain top talent.
- Create partnerships with local educational institutions: Local community colleges and universities that offer cybersecurity programs serve as excellent sources for new talent. Additionally, these institutions provide opportunities to enhance the skill sets of current employees. Cybersecurity apprenticeships, cyber range simulation training, blue-teaming competitions and various other proactive educational initiatives can help uplevel the workforce.
- Foster relationships with cybersecurity consultants to bridge the skills gap: Retention is challenging, so establishing collaborative relationships with reputable cybersecurity firms provides organizations with access to specialized expertise and resources, helping to

address the shortage of cybersecurity professionals. And if designed appropriately, these relationships offer the benefit of independent perspectives and impartial assessments, allowing executives to make informed decisions and navigate complex cybersecurity challenges with confidence. This also alleviates pressure on security teams, allowing them to focus on core responsibilities with greater confidence.

- Invest in new technologies: New innovations make cybersecurity professionals' lives easier and enable them to focus more on high-value activities like the cybersecurity training of business users. For example, investments in AI-powered solutions can automate the monitoring of security logs. They can also generate alerts when devices connected to the network behave suspiciously. Such technologies augment any organization's security stance and free cybersecurity employees from tasks that, while important, can be tedious.

The greatest vulnerability in many organizations today is the inability of leaders to communicate and collaborate on their cybersecurity needs and investments. In years to come, those who develop strong personal relationships in the cybersecurity community will possess an asset that will only grow more valuable with time – an experienced, proven, satisfied and dedicated cybersecurity team – teams of professionals that will increasingly be required not only to secure cybersecurity insurance, but to successfully complete the digital transformations required for business success.

https://www.securitymagazine.com/articles/100608-bridging-the-widening-cybersecurity-skills-gap