The Cybersecurity Talent Gap Is An Industry Crisis

Forbes
Technology
Council

POST WRITTEN BY

Brian NeSmith

Brian NeSmith is the CEO and Co-Founder of **Arctic Wolf Networks**, a leading SOC-as-a-service company, based in Sunnyvale, CA.

If you're finding the job market a bit tight these days, you must not be in cybersecurity. As hackers ramp up attacks with increasingly sophisticated methods and tools that are readily available for purchase on the dark web, the "white hats" need all the help they can get. According to recent estimates, there will be as many as 3.5 million unfilled positions in the industry by 2021.

This puts many organizations in a tight spot, as security engineers are hard to find and command top salary figures when available. Cybercriminals, of course, aren't complaining. They're doing everything

they can to take advantage of understaffed firms that have little ability to prevent, detect and responds to attacks. These companies are at high risk of suffering a data breach that may take years to recover from.

How Did We Get Here?

With digital transformation and the ubiquity of web and cloud applications and services currently offered, it's hard for businesses to fill many of their information technology (IT) positions, let alone ones that require security expertise. Another problem: Smaller enterprises find themselves more frequently targeted -- sometimes as a conduit to their larger partners and customers. While specialized security experts quickly get snatched up by large corporations, other companies need to tap into such expertise too, and they need them now: According to the 2017 Global Information Security Workforce (GISW) Study, two-thirds of its nearly 20,000 respondents indicated that their organizations lack the number of cybersecurity professionals needed for today's threat climate.

Companies need to broaden their range of potential candidates to seek smart, motivated and dedicated individuals who work well as part of a team. Just because they may not have the degrees, certificates or prior experience a company might hope for doesn't mean they won't be an excellent fit. If they're smart, collaborative and like to solve problems, it might make sense to consider their potential.

Women to the rescue? By and large, men dominate the cybersecurity job market. In fact, estimates say women only make up 14% of the U.S. cybersecurity workforce. With the ongoing attention and heightened urgency regarding the industry's skills shortage, that needs to change. Firms must encourage more women applicants and recognize existing bias in hiring practices. Interestingly, coding clubs and cybersecurity camps for girls are becoming more common so that one day they can break men's stranglehold on the profession, but "one day" is still a long way off.

Ex-military serving on a new battlefield? Another pipeline that may help close the skills gap comes via former military service personnel. Whether through the public or private sectors, cybersecurity job opportunities present themselves to military veterans. Much of the situational, hands-on experience of veterans translates well to the battlefield of cybersecurity. Today, many veterans' programs are promoting opportunities in the industry and providing cybersecurity training and certifications to a growing number of interested veterans.

Technical expertise can be learned. About three in ten cybersecurity professionals came to the field from a background outside of information technology. The 2017 GISW Study found that 33% of cybersecurity executives arrived in the industry via non-technical careers. There can be a disconnect between hiring managers' and candidates' expectations. While many candidates may not feel qualified for a position for lack of technical skills, most hiring managers prioritize communications and analytical skills, understanding that new employees will rapidly acquire technical skills as they gain experience.

Technology Helps, But Only So Much

Even if the pipeline sees a massive uptick in non-traditional candidates, the skills shortage in cybersecurity won't end anytime soon. For that reason, companies seek alternative solutions wherever they can find them. Many look to the promise of big data, artificial intelligence (AI) and machine learning as a way to bridge the gap.

Humans can only process so much information in a short amount of time. Machine learning-based security solutions, however, can handle billions of security events in a single day -- finding possible threats early on through a combination of correlation, pattern matching and anomaly detection. The catch is that while the technology enables you to detect more threats faster than ever before, the alerts it produces still require investigation and analysis to determine their legitimacy and, when more threats are detected, more cybersecurity professionals are required to respond to and hunt down these threats.

On one hand, these solutions give you an excellent opportunity to improve your organization's security posture, but only by adding a number of skilled security engineers and analysts to your existing IT team. The skills gap for these positions is a chasm the size of the Grand Canyon. According to Dark Reading's report (registration required), only 14% of IT security managers feel there are currently enough cybersecurity professionals in the field with the needed skills to hunt down and respond to threats.

One Possible Solution

There's no end in sight for the skills gap crisis, so organizations must look at the problem in new ways. The quickest solution would be for one person to be able to do the work of five, and AI makes that possible. It's just that the "one" employee must be a skilled security expert of the highest caliber, someone able to quickly assess, triage and address the threats that put your business at risk. Yet, such technology is complex and burdensome, and such skilled expertise is nearly impossible to find. So, what are organizations to do?

Solving this problem requires a different way of thinking; organizations can't just rely on technology alone. The talent crisis is real, and as an industry, we can't wait years for a solution. The good news? An emerging set of companies are outcome-focused and look at people, processes and technology holistically. This means getting more out of your existing security resources, not just adding more. Companies can't do everything themselves. They must use or augment their internal resources with those of security service providers. The companies that realize this will lay claim to the most robust security and avoid the disastrous consequences of a major cybersecurity breach.