TD SYNNEX

The Cybersecurity Skills Gap

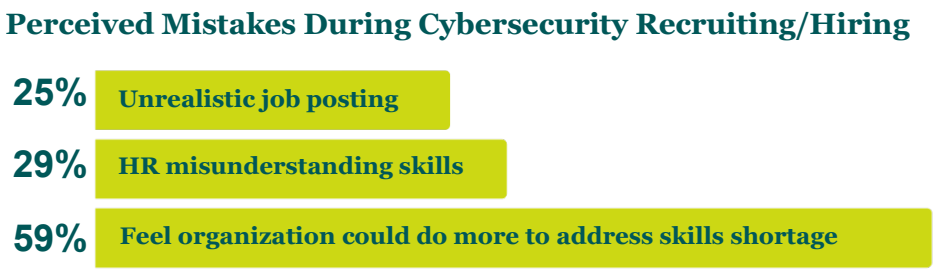
What It Is, Its Impact and How To Bridge the Gap

What Is the Cybersecurity Skills Gap?

Simply put: there aren't enough skilled individuals to fill cybersecurity positions. In 2021, there were an estimated 3.5 million open job requisitions for cybersecurity professionals globally – with 465,000 in the United States alone. Unfilled job requisites increased 350% from 2013, and it's predicted that the same number of open positions will remain through 2025.[1]

A handful of factors have contributed to the cybersecurity skills gap, which has been on the industry's radar for roughly the past decade. Job postings with misaligned requirements are one reason cybersecurity positions go unfilled. How can an entry-level analyst hold certifications that take multiple years to achieve? And similarly, how can a job prospect have 10 years of experience working with a specific technology that was developed less than five years ago?

Cybersecurity can also attract 'non-traditional' candidates, whose expertise has been developed outside of a classroom or through hands-on experience, whose applications can become hindered by inflexible degree requirements. Similarly, requiring stringent criteria for cybersecurity positions, including multiple certifications or extensive experience, can also limit a position's applicant pool.



Recent ESG and ISSA research, captured from a survey of 489 cybersecurity professionals, highlights mistakes when hiring cybersecurity talent. While supply and demand plays an important role, the findings show many believe their organizations contribute to the skills gap: 29% of respondents said their organization's HR department doesn't understand the requisite skills,

[1] Cybersecurity Jobs Report: 3.5 million openings in 2025. Cybercrime Magazine. Nov. 9, 2021. https://cybersecurityventures.com/jobs/

and 25% indicated job postings were unrealistic. Nearly 60% of respondents "felt their organization could be doing more to address the cybersecurity skills shortage."[2]

In addition to the shortage of qualified cybersecurity professionals, ESG and ISSA research also indicates another lesser-discussed implication in the cybersecurity skills gap: currently-employed cybersecurity professionals who "lack the advanced skills necessary to safeguard critical business assets or counteract sophisticated cyber-adversaries." [3]

The Cybersecurity Demand Gap

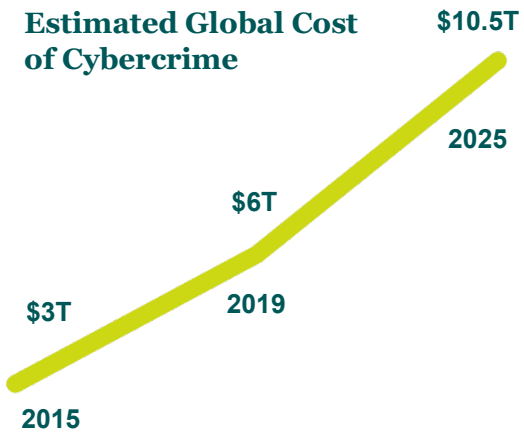
The increasing number of cyberattacks on organizations of all sizes is driving demand for cybersecurity personnel. The demand gap, also referred to as the cybersecurity workforce gap, is created because the need for cybersecurity professionals outweighs the supply of qualified individuals. The cybersecurity skills gap hurts those in the cybersecurity workforce. ESG and ISSA findings show 57% of organizations are impacted by the skills gap – leading to a heavier workload and burnout among staff.[4]

Criminal and nation-state sponsored hacking has grown rapidly and increased in sophistication, while academic curriculum is still relatively new and emerging, and education and training outlets in the U.S. have found it challenging to progress at the same rate as the growing threatscape.

[2],[3] ESG RESEARCH REPORT: The Life and Times of Cybersecurity Professionals 2021, Volume V. A Cooperative Research Project by ESG and ISSA, July 2021. https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

[4] The Life and Times of Cybersecurity Professionals 2021. July 2021. https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

The estimated global cost of cybercrime in 2021 was $6 trillion, and it's expected to rise to $10.5 trillion by 2025.[5] For additional perspective, cybercrime was estimated at $3 trillion in 2015.



Meanwhile, almost two-thirds of cybersecurity professionals believe their organizations are understaffed. Cybersecurity staff shortages have major consequences.

Responses to the ISC(2) 2021 Cybersecurity Workforce Study illustrated the ramifications to their organizations from having understaffed cybersecurity departments:

- **32%**: misconfigured systems
- **30%**: not enough time for proper risk assessment and management
- **29%**: slow to patch critical systems
- **28%**: process/procedure oversights
- **27%**: inability to remain aware of all threats active against our network
- **27%**: rushed deployments[6]

Bridging the Gap

There are a handful of ways those in the industry can help address – and bridge – the cybersecurity workforce gap.

While the main focus of cybersecurity education and training is technical aptitude, curriculum should also help develop students' soft skills. Possessing soft skills, such as teamwork, communication and collaboration, helps cybersecurity professionals translate their technical knowledge into value for their employer.

[5] Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Nov. 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
[6] A Resilient Cybersecurity Profession Charts the Path Forward (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021 ISC2-Cybersecurity-Workforce-Study-2021.ashx

A study conducted by Tripwire also showed that possessing soft skills is highly valued by security teams: every survey participant thought soft skills were important when hiring, and top soft skills desired included analytical thinking and good communication.[7] Additionally, data from (ISC)2 indicates that the most important non-technical qualifications for cybersecurity professionals are:

Strong problem-solving abilities (38%)

Strong communication skills (32%)

Curiosity and eagerness to learn (32%)

Strong strategic thinking skills (23%)[8]

Hiring managers should take note: the cybersecurity industry wants these valuable non-technical qualities from job applicants, and that increasing the importance of these attributes can potentially increase the security talent pool.

A diverse team can also be key to bridging the gap. Diverse teams foster creativity and introduce different perspectives, that can help with problem solving and troubleshooting issues. While the industry remains largely male (76%) and Caucasian (72%)[9] in North America and the U.K., hiring managers have an opportunity to broaden their hiring networks and search in less traditional outlets to improve diversity within their security teams.

Impact on the IT Community

Many managed service providers (MSP) and value-added resellers (VAR) have been providing a variety of products and services to customers to improve their IT operations for decades. These organizations are on the front lines of today's cyber threats.

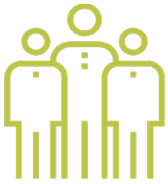
While the cybersecurity demand gap impacts nearly every organization, its impact is felt by MSPs and VARs daily. To remain relevant and competitive in the IT services market, today's

[7] Survey Says: Soft Skills Highly Valued by Security Team. Oct. 17,2017. https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/
[8] A Resilient Cybersecurity Profession Charts the Path Forward (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021 ISC2-Cybersecurity-Workforce-Study-2021.ashx
[9] (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

MSPs and VARs need to have a comprehensive approach to promoting and delivering cybersecurity solutions.

MSPs and VARs should invest in training and education for their teams to address the skills gap impacting their customers. Expanding a team's skill set can widen an organization's overall technical expertise and open the door to new business opportunities.

But which particular training is most important? Organizations can identify cybersecurity market opportunities and compare those with their internal skills gap, and focus on reducing or eliminating those deficits. Providing training in broad brushstrokes is also smart; training should expand beyond the technicians and engineers – marketers, sales professionals and even owners can benefit from relevant training. MSPs and VARs can also identify the certifications their clients consider vital.



More than half of employees believe their employer should provide opportunities for personal growth. [11]

There's a financial – and intrinsic – benefit to training your workforce, too. An engaged workforce is a more productive workforce, and organizations that focus on employee development experience increased sales and profits[10]. According to Gartner, a majority of employees feel it's important for their organization to provide opportunities for personal growth[11]. People are motivated when they feel valued, and growth opportunities that help improve their sense of personal value and purpose can help achieve that enthusiasm.

Additionally, research from Cornell University's ILR School indicates that investing in training helps increase employees' value to an organization, and that companies who invested more in training prior to the Covid-19 pandemic were less likely to reduce their staff numbers in order to cope with pandemic-driven financial burdens[12].

[10] Global Study: ROI for Strengths-Based Development. Sept. 22, 2016. https://www.gallup.com/workplace/236288/global-study-roi-strengths-based-development.aspx
[11] Gartner HR Research Shows Organizations Must Reinvent Their Employee Value Proposition to Deliver a More Human Deal. May 25, 2021. https://www.gartner.com/en/newsroom/press-releases/2020-05-25-gartner-hr-research-shows-organizations-must-reinvent-their-employment-value-proposition-to-deliver-a-more-human-deal
[12] Investing for Keeps: Firms' Pre-Pandemic Investments in Human Capital Decreased Workforce Reductions Associated With COVID-19 Financial Pressures. Nov. 17,2021. https://news.cornell.edu/stories/2021/11/employee-training-pays-fewer-layoffs

The TD SYNNEX Passage Program

The cybersecurity skills gap and demand gap illustrate the need for organizations to continue to train and upskill their existing security professionals and have specific – but realistic – expectations when hiring new team members.

While there are online bootcamps, programs and resources dedicated to cybersecurity, many don't provide a truly comprehensive approach, bundling technical expertise with sought-after soft skills.

The recently launched TD SYNNEX Passage Program, is a professional service designed to develop both upcoming and established cybersecurity professionals. The program addresses the cybersecurity skills gap through two tracks, the Placement Initiative and the Upskill Initiative:

The Placement Initiative is designed to place candidates into new job roles by providing the resources and technical skills needed to succeed in cybersecurity. This includes skills ranging from investigating alerts to report writing. Candidates are provided with skills training, industry knowledge, career consulting, a final assessment of job readiness, and receive placement assistance into a cybersecurity job role.

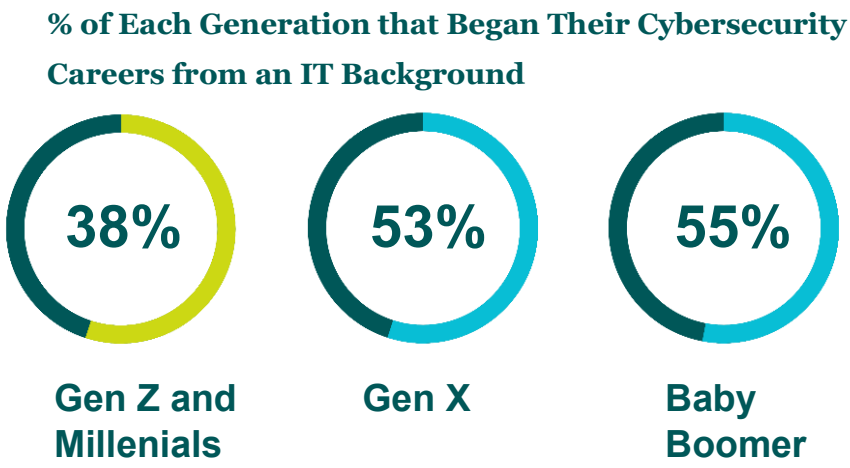
The Upskill Initiative is designed to develop currently employed cybersecurity professionals in their roles by providing the resources and competencies to enhance and build upon existing technical skills. The Passage Program staff and trainings eliminate the hassle of needing to spend time and resources towards developing the right cybersecurity candidate to fit the right role.

The initiatives support job readiness and development for **Cybersecurity Analyst** and **Junior Penetration Tester** roles. While both initiatives focus on the same roles, they are directed towards an individual's current skill and experience level. These roles were chosen based on their relevance and importance in the industry: a Cybersecurity Analyst is a core job role in defensive cybersecurity, and a Junior Penetration Tester is the entry level job role into offensive cybersecurity.

New Pathways to Cybersecurity

The Passage Program is also a critical resource for current professionals who want to learn modern-day trends and technical methodologies, but may be several years removed from their formal education.

ISC(2) research shows that pathways leading to cybersecurity careers are changing, with more entry points into the industry emerging: 17% of cybersecurity professionals surveyed transitioned from unrelated career fields and 15% gained access through cybersecurity education[13]. That same research showed that while starting a career in IT was the traditional path into a cybersecurity career, more people are segueing into the industry from diverse paths. Of Gen Z and Millennials (ages 39 and under), only 38% started in IT, compared to 53% of Gen X (ages 39-54) and 55% of Baby Boomers (ages 55+).



The Passage Program offers an opportunity for those interested in beginning their career in cybersecurity, and conversely keeping those currently employed in cybersecurity at the top of their game. The Passage Program also offers critical soft skills resources, designed to better prepare candidates for the workforce, including resume building and interviewing. These soft skills may not be addressed in other programs.

[13] ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Closing the Gap

"Can we produce enough appropriately skilled defenders of digital systems to defeat threats that range from natural disasters to user errors, from product defects to a growing cast of 'bad actors' who seek to compromise such systems for nefarious and often criminal purposes?"[14]

This question helps reveal the extent of the global cybersecurity skills shortage. There is no overnight solution to address the workforce demand gap, but incremental change can help bridge it.

For more information on the TD SYNNEX Passage Program, visit our website or email us at TDCRPassage@techdata.com.

For blog posts on the cybersecurity skills gap, view our Medium blog.

[14] MIND THIS GAP: CRIMINAL HACKING AND THE GLOBAL CYBERSECURITY SKILLS SHORTAGE, A CRITICAL ANALYSIS Stephen Cobb ESET, USA Cobb-VB2016-from1.indd (archive.org)