CyberTalk.org

A Guide to Closing the Cyber Security Talent Gap

TABLE OF CONTENTS

INTRODUCTION

Will your organization see cyber security success despite today's unprecedented cyber security talent shortage?

It's no secret. Top talent is notoriously tough to find. And the issue is turning into an industry crisis.

Only **30%** of organizations say that they retain adequate cyber security staffing.[1] Fifty-percent of organizations that report staffing shortages say that they remain at a 'moderate' or 'extreme' risk of a cyber attack. And roughly **3.5 million** global cyber security positions are going unfilled.[2]

Organizations need more talent to join cyber security staff. But how can they make it happen?

> "Even if we had unlimited funding to go hire the best people, there just aren't enough best people."
>
> – Workforce Security Expert, Brian Linder

[1] Help Wanted for 3.4M Jobs: Cyber Workforce Shortage is an Acute, Worldwide Problem, David Jones, Cybersecurity Dive, Oct 24, 2022
[2] A New Approach is Needed to Close the Cybersecurity Talent Gap, Rami Sass, Forbes, Nov 14, 2022

DYNAMIC TRENDS: HOW DID WE GET HERE?

One of the earliest mentions of the cyber security talent shortage occurred in 2011, when ESG analyst John Olsik pondered, "Will there be a shortage of cyber security professionals in 2011?" The same topic continually resurfaces in business conversations nearly 12 years later.[3]

Historically, other burgeoning industries have encountered similar difficulties. The oil industry, the construction industry, the logistics sector and others have all experienced growth spurts and labor shortages that have led to high levels of competition for talent—if not all-out talent wars.

Smart businesses are recognizing that the cyber security talent shortage affects economies, entire populations' welfare, along with political agendas, and peacekeeping efforts.

Private sector businesses and government organizations are taking steps to address this stressor, but precisely how it's handled could affect the success and failure of organizations, along with the lives and livelihoods that depend on reliable cyber security.

[3] Will There Be A Shortage of Cyber Security Professionals in 2011?, Jon Oltsik, CSO Magazine, Jan 3, 2011

MYTH VS. FACT

IS THE TALENT SHORTAGE A MYTH?

In some corners of the internet, articles have appeared stating that the cyber security talent shortage is a myth. At CyberTalk, we believe that the talent shortage is not a myth, although there are factors within organizations' control that influence its continuation and severity.

An analyst report found that cyber security staffing shortages were made worse by biases in hiring, inadequate compensation offered, and ineffective hiring processes.[4]

[4] Security & Risk 2019: Cybersecurity's Staffing Shortage Is Self-Inflicted, Joseph Blankenship, Forrester, Aug 6 2019

WHAT'S NEXT?
A PROACTIVE APPROACH

Discover how to start solving the issue that is the cyber security talent shortage.

As cyber attacks become increasingly commonplace and complex, organizations need to reassess and revise talent acquisition and retention strategies, if any at all are in place.

1

In the past, hiring for cyber security has commonly relied on a top-down approach, where the senior-most positions are filled first, and lower-ranking positions are filled later. However, worker shortages and the need to fulfill specific technical roles renders this hiring model only somewhat effective and some might argue that it's outdated.

Analyst firms suggest that organizations consider a talent-to-value approach, which reduces risk associated with hiring, and focuses on new and existing talent development. The talent-to-value model can work in any of a variety of different ways, depending on where an organization is in its security journey. In essence, talent-to-value focuses on meeting business needs in the moment, and mitigating risks based on priority and risk appetite.

2

Organizations that prioritize inclusive hiring practices are likely to see significant payoff. Make Diversity, Equity and Inclusion (DEI) a KPI for your security team. Although some are quick to assume that DEI as a specific KPI is unrealistic, organizations with more diverse executive teams are 25% more likely to achieve above-average profitability levels. Diverse teams are stronger teams. In sum, DEI outcomes can be tied to effectiveness and profits.

As your organization recruits diverse talent, ensure that leaders also become champions of diverse talent, serving as advocates for new hires and offering mentorship. Foster a supportive and inclusive company culture that effectively supports all hires.[5] Take the time to upskill talent so that they are well-equipped with skills they'll need in the future.

[5] Fix the Vulnerability Within: Break Gender Bias in Cybersecurity, Forbes, March 9, 2022

81% of organizations report that the skills required to be a "great" staff member had changed in the past several years.[6]

3 Ensure that your organization's compensation offerings are competitive. In the U.S., cyber security salaries commonly range from $85,000 to $130,000. However, on account of the talent shortage, and as candidates have gained leverage in the hiring process, some U.S. companies are offering as much as or upwards of $200,000.

4 Cyber security recruitment efforts tend to focus on candidates with traditional educational backgrounds. However, many talented cyber security professionals enter the field through non-traditional paths.

People without high school or college degrees, or even technical backgrounds, can make good cyber security hires. Selecting non-traditional candidates requires focusing on potential, motivation and analogous experience.

5 Retain a pipeline of emerging security leaders. When filling internal cyber security leadership roles, organizations should strive to promote from within. This helps with middle management retention, as it shows relevant individuals that there is a clear and attainable career path, and supports the longer-term sustainability of the security team.

Security leadership may wish to work with the HR team to define key leadership competencies required within the organization. Afterwards, existing leadership may wish to conduct a skills assessment across the IT workforce, with a baked in leadership competency evaluation. This can assist everyone in identifying staff with leadership potential; staff who may be strong candidates for future leadership roles.

[6] Cyber Talent Gaps Force IT Security Employers to Hire Creatively, Ryan Golden, HR Dive, Sept 14, 2017

6 Offer existing cyber security talent best-in-class training. Advancing the skills of emerging and exceptional tech talent will help organizations more easily address future cyber and IT challenges. Learning opportunities presented in the form of 'small bites' of information can be effective, or organizations may wish to extend opportunities through more formal programs like Cybrary, or Mind, among others.

7 Finally, interest in career paths tends to start at an early age. It's time to think about how to encourage interests in computing and cyber security in elementary school. By the time that some students reach middle and high school, they have already decided on career paths. As students increase their knowledge and seriousness around pursuing a security career, industry needs to provide appropriate internships and talent-to-hire programs. *On the next page, Check Point's Global CISO, Jonathan Fischbein shares his perspectives on this very topic.*

EXPERT INSIGHTS HIGHLIGHT

Jonathan Fischbein
Global CISO, Check Point

“There is a shortage of skilled person-power in cyber security and budgets are not increasing at the speed of attacks. I truly believe that industry may need to foster high school programs to begin training students in their high school years. Security teams also need to recruit students early in their university years, placing them in security internships.”

“Today most security practitioners finish university and then start as entry level employees. However, unfortunately, most organizations want to hire practitioners with 2-4 years of experience. So this is a huge challenge.”

“We need to develop stronger strategies to cultivate, attract, train and employ the next generation of security professionals.”

CONCLUSION

Developing a complete and competent cyber security team amidst a talent shortage is challenging, but possible. It requires taking bold leaps. Organizations may need to be creative when it comes to finding the next cyber security hire.

Leverage evidence-based approaches to expand your cyber security workforce and protect your organization in entirety. At the end of the day, your talent is at the heart of a cyber secure and cyber-resilient organization.

Interested in additional cyber security workforce management insights?
Learn more on [CyberTalk.org](https://www.cybertalk.org).

> At the end of the day, your talent is at the heart of a cyber secure & cyber-resilient organization.