TalPoint

The 2023 Compliance and Cybersecurity Talent Marketplace Guide

The cybersecurity talent deficit is a serious problem for companies. Learn how you can address this problem with proven strategies and a talent marketplace.

Table of Contents

Introduction

The growing cybercrime epidemic is causing sleepless nights for enterprise leaders everywhere. And no wonder, considering that almost half (45%) of companies in the U.S. suffered a data breach and 24% of companies in Europe and the Middle East experienced a ransomware attack in 2021. These numbers explain why Gartner discovered that for 88% of company boards, cybersecurity is not just a "technical" IT problem, but a serious business risk.

A vast number of these breaches (82%) involve the "human element". Furthermore, there were 13% more ransomware breaches in 2021 – more than in the previous 5 years combined. Supply chain intrusions have also increased in recent years.

Unfortunately, this is not all that organizations have to worry about.

Not only are cyberattacks happening more frequently, they are also costing organizations a lot more than they did in the past. According to IBM's 2022 cost of a data breach report, the average cost of a single breach has now reached a record high of US$4.35 million. For US companies, the cost is more than double at US$9.44 million.

To prevent breaches and avoid these potentially astronomical costs, companies need well-prepared cybersecurity teams populated with skilled cybersecurity professionals. Unfortunately, the cybersecurity industry is grappling with a talent shortage, with one study revealing that 63% of respondent organizations have unfilled cybersecurity positions and 60% experiencing difficulties retaining qualified cybersecurity personnel.

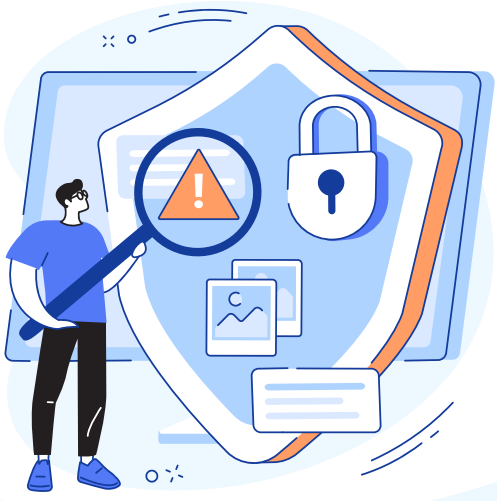
What can you do to address the problem, add the right resources to your team, and strengthen your cyber defenses?

The Talent Shortage Problem in Cybersecurity

> **The cybersecurity skills crisis continues on a downward, multi-year trend of bad to worse.**
>
> *-Information Systems Security Association International (ISSA).*

This same sentiment is echoed by many security experts and researchers worldwide. It's not easy for organizations to find skilled cyber professionals because there simply aren't enough of them. Between 2013 and 2021, the number of unfilled cybersecurity jobs grew from 1 million to 3.5 million – a 350% jump. The same number of openings will still be available in 2025 according to some experts.Others believe that the gap will widen even further with the demand for certain cybersecurity practitioners increasing faster than supply can keep up. For instance, the U.S. Bureau of Labor Statistics (BLS) predicts that the demand for information security analysts will grow by 35% between 2021 and 2031, much faster than the average for all occupations.

ISACA's State of Cybersecurity 2022 report also highlights how organizations are struggling to hire and retain skilled compliance and cyber professionals. It's why 62% of cybersecurity teams are understaffed, why 63% of companies have unfilled vacancies, and why 60% have experienced difficulties retaining qualified staff.

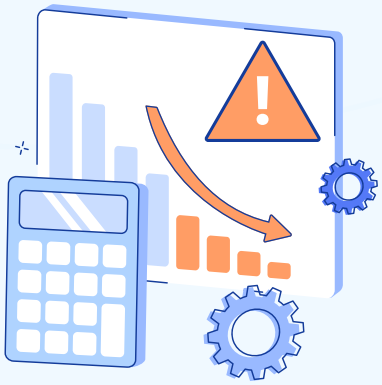


According to one McAfee report, the cybersecurity talent shortage is a challenge in all sectors, particularly because it exacerbates the already difficult task of cybersecurity risk management and mitigation. Furthermore, due to shortages:

- The workloads of existing cybersecurity teams are increasing
- Critical skills gaps on cybersecurity teams mean workers are having to take on roles and responsibilities they're not always trained to do
- There are more unfilled job requisitions
- The burnout rate among staff is very high
- Organizations become more attractive hacking targets
- Companies struggle to strengthen their cybersecurity programs, particularly in the areas of intrusion detection, software development, and attack mitigation

Many companies now view cybersecurity as a critical imperative. Still others believe that a strong cybersecurity program can be a strategic growth driver. However, they struggle to strengthen these programs because they are unable to address the skills shortage problem.

The Root Causes of Cybersecurity and Compliance Talent Shortages



Organizations that are aware of compliance and cybersecurity risks recognize the value in recruiting top talent. But this doesn't necessarily mean that they can because as we have already seen, the demand for skilled cybersecurity – and for that matter, compliance – professionals far outstrips the supply.

There are multiple reasons for these shortages:

01 Cybersecurity is not promoted as a career path to youngsters

Countries are not making enough of an effort to "evangelize" cybersecurity at the K-12 level. Simply put, they are not starting young. To get more people to pursue cybersecurity careers, it's important to encourage their interest right at the school level through cybersecurity education programs, mentorship, and awareness campaigns.

02 Organizations' insistence on degrees

Many companies insist on only hiring professionals like computer science graduates. Such inflexibility leaves out many candidates who don't hold these degrees but otherwise have the skills or experience that could be really valuable in real-world cybersecurity settings. Insisting on certifications can also become problematic if the holder doesn't also have the requisite experience or skills.

03 Lack of training and personnel oversight

Training and oversight are important to ensure that cybersecurity team members are applying their skills in the right way. But when team managers are already overwhelmed keeping up with the burgeoning threat landscape, it's difficult for them to find the time to train new staff or oversee them in their day-to-day jobs.

These gaps may result in personnel feeling disconnected on the job and not having the appropriate mentorship to develop critical skills to be successful in their roles.= In some cases, lack of training or a shortage of new learning opportunities may contribute to them feeling burned out and quitting right when their companies need them the most.

04 Lack of diversity

Diversity is one of the biggest problems contributing to the talent shortage. For example, in 2021, women represented only 25% of the global cybersecurity workforce. And while this is significantly better than the 11% they represented in 2011, more women are needed to fill cybersecurity jobs in the coming years in order to shrink the skills gap. In general, a more diverse cyber workforce is essential to increase an organization's cybersecurity and compliance talent pipeline.

05 Flat learning curve

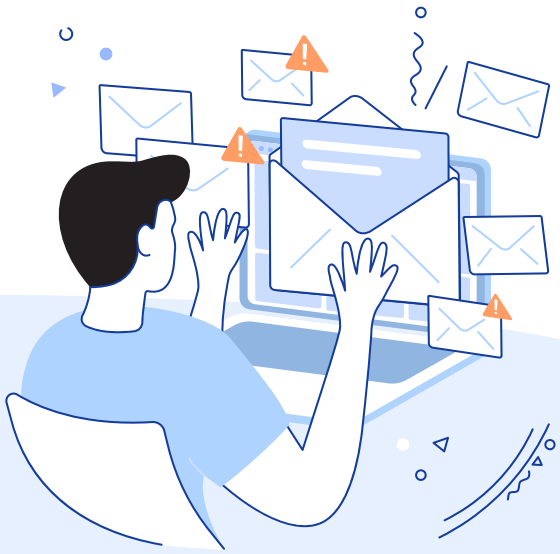
Cyberthreats are evolving rapidly and cyberattackers are getting more sophisticated by the day. But the people who can fight these threats are struggling to keep up. According to one report, it takes around two years for an entry-level cybersecurity employee to create value for the organization. This period is too long in an era where threats can come from everywhere and at any time.

06 Existing teams are overworked and stressed

The lack of a talent pipeline means that existing teams are under a lot of pressure to manage organizations' security and legal compliance programs. Alert fatigue is also a real problem because incident responders spend 2.5-5 hours each day only on alert investigations.

For all these reasons, cybersecurity team members are overworked, stressed, and in some cases, burned out. These facts explain why:

- Stress negatively impacts the ability of 90% of security personnel to do their jobs
- 65% of cybersecurity analysts and 46% of senior professionals have considered quitting their jobs
- 42% of Chief Information Security Officers (CISOs) are suffering from cybersecurity fatigue
- 34% of cybersecurity leaders say that it's difficult to recruit staff following an attack
- 24% of Fortune 500 CISOs stay on the job for just one year



The Cybersecurity/Compliance Talent Challenges That Lie Ahead

As security threats increase and skills shortages continue, organizations should be prepared for these challenges that lie ahead:

Budget constraints

According to Gartner, the global spending on cybersecurity was $158 billion in 2021. By October 2022, this figure had increased to $169 billion. The upward-moving trend will continue in 2023, with Gartner predicting that organizations will spend over $188 billion on information security and risk management products and services.That said, many companies still have small budgets for cybersecurity and compliance hiring and thus struggle the most when it comes to recruiting top talent.

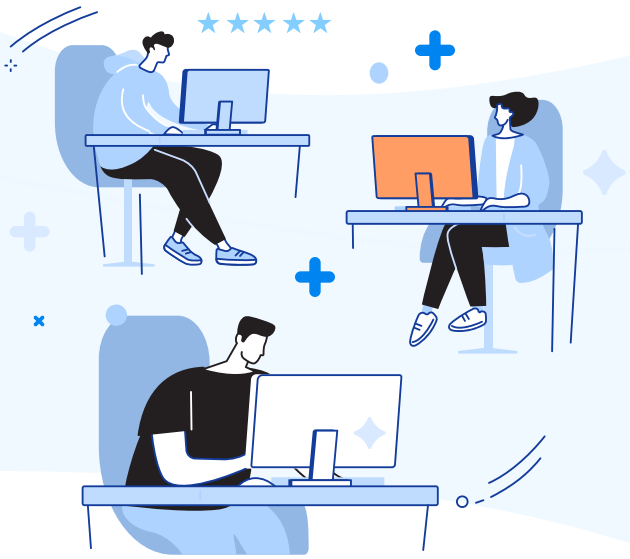
But companies with larger hiring budgets and growing companies also have to deal with some challenges. For one, they become more vulnerable as they grow because they have more employees, processes, and third-party vendors, utilize more tools, interact with many other organizations, and tend to suffer from more tech debt – all of which opens new attack pathways for cyberattackers. Often, large companies also struggle to effectively combine human talent, work processes, and robust cybersecurity technology and tools due to which they too find it hard to uncover vulnerabilities, conduct risk assessments, and strengthen incident response. Some firms also labor to maximize their cybersecurity budgets in order to hire the best talent and improve their security posture.

Increasing compliance complexity

The compliance landscape is becoming increasingly complex both due to regulatory burdens as well as customer expectations. Companies may not always be able to keep up with the various frameworks and standards that have evolved in recent years. In order to protect the enterprise and maintain strong cybersecurity and compliance, they will need people who understand these standards and can streamline compliance processes – which again, is not easy to do. Firms without compliance experts will lose more deals, potentially experience customer churn, and see weaker bottom lines.

Salaries are going up for talented professionals

The talent demand-supply gap means that salaries for skilled cybersecurity and compliance professionals are getting bigger. For example, per one report, the average salary of Cybersecurity Analysts in the U.S increased by 16.3% between 2020 and 2021. Again, companies that cannot match these expectations will lose out in the hiring race to competitors.



How the World Is Tackling Cybersecurity Skills Shortages

Many companies are scaling up their efforts to tackle the cybersecurity skills shortage. Some are working with staffing and recruitment agencies, while others are partnering with certification organizations, schools, universities, and government workforce programs. Another increasingly-popular avenue is to sign up on talent marketplaces like TalPoint that enable companies of all sizes to source experts in security, privacy, risk and compliance.

Many larger companies are also leading efforts to grow the global cybersecurity workforce. For example, in 2021, Microsoft launched a campaign to expand the U.S. cybersecurity

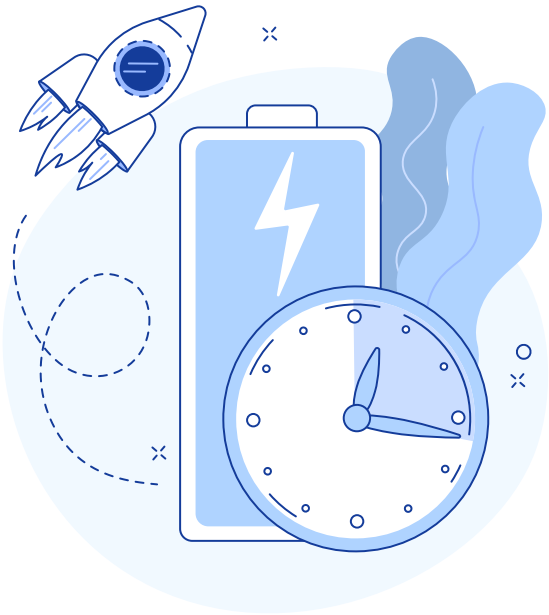
workforce by 2025. The company will work with U.S. community colleges to help place 250,000 people into cybersecurity jobs, not only at Microsoft, but also at tens of thousands of other employers in the country.

Similarly, Deloitte has started a global awareness and recruitment campaign to attract more women into the cyber profession. Search engine giant Google has pledged to teach 100,000 Americans in-demand skills like data privacy and security through the Google Career Certificate program. IBM has also announced its intentions to train 150,000 people in cybersecurity skills by 2024. They will also partner with numerous colleges and universities to establish cybersecurity leadership centers and ultimately, grow a more diverse cyber workforce in the USA.

Other organizations are also joining the effort to expand the cybersecurity workforce according to a 2021 fact sheet by The White House. This includes code.org who have pledged to teach cybersecurity to over 3 million students over 3 years, Girls Who Code who will provide scholarships and early career opportunities to underrepresented groups in technology (e.g., women), and the University of Texas that has committed to developing new short-term credentials in cyber-related fields

Non-profits have also joined the talent-finding effort. One is the Cyber Talent Institute (CTI) that aims to eliminate the cybersecurity talent shortage in the U.S. within seven years. In 2021, the group held the inaugural Cyber Talent CIO Forum where technology, business and cybersecurity leaders committed to discover and train 25,000 cyber stars by 2025.

One of the biggest advantages of talent marketplaces is that they do all the hard work of sourcing, vetting, selecting, and onboarding the best possible talent. Companies also have the added benefit of past client experience in the form of ratings and reviews. Moreover, they always focus on the company's specific requirements so the chances of misfits are very low.



Strategies to Attract Cybersecurity Talent and Overcome the Shortage

In its 2021 annual global study of cybersecurity professionals, ISSA said that the cybersecurity skills crisis has impacted more than half (57%) of organizations worldwide. The good news is that you can attract talented cybersecurity and compliance professionals to your organization. Try these proven strategies!

01 Implement training programs

You can close the cybersecurity/compliance skill gap by implementing and appropriately funding training programs. Training is essential to help new entrants start making tangible contributions almost immediately, and to empower experienced professionals to advance their skills and match the organization's cybersecurity or regulatory compliance requirements.

02 Revisit compensation packages

The ISSA report found that inadequate or below-par compensation is the biggest factor (38%) contributing to the talent shortage problem. Revisit your compensation packages and research average salaries for the professionals that you need. If required, lobby the C-Suite to increase your cybersecurity personnel budget.

03 Look for skills and expertise, not just degrees

As we saw earlier, organizations that insist on degrees or certifications often lose out on many talented candidates who can bring a lot of value to cybersecurity and compliance programs. Prioritizing skills, knowledge, experience, and personal qualities like situational awareness and resilience are much better measures of talent than college degrees.

04 Adjust expectations during recruitment

In the ISSA study, 25% of professionals said that the cybersecurity-related job postings at their organizations are unrealistic. Another 30% also said that recruiters must be educated on the company's cybersecurity goals.

As the demand for talent increases, recruiting managers must adjust their expectations, rethink the skill sets and credentials they want, and avoid looking for non-existent "unicorns" (aka perfect candidates).

It's also important to balance hiring across entry-level and experienced candidates. The latter are harder to find and more expensive. Plus, practitioners who are at an earlier stage in their careers juniors can fill many roles with appropriate onboarding and training. Strong oversight and leadership can also bring them up to speed to match the cybersecurity team's – and thus the organization's – requirements.

05 Sign up with a talent marketplace

A talent marketplace like TalPoint is a good place to find security, compliance, risk management, and data privacy experts. The best marketplaces have a network of qualified professionals and can help you source the right talent for your specific project, cybersecurity objectives, compliance goals, and IT infrastructure.

Hire Cybersecurity and Compliance Experts with TalPoint

As the threat landscape expands, your organization needs a robust workforce of skilled and knowledgeable cybersecurity and compliance personnel. And you can bring in these people into your ecosystem through training and education and diversity initiatives. You can also build your own talent pipeline to defeat threat actors and create a more secure environment. How? By signing up with a talent marketplace like TalPoint.

TalPoint is the only talent marketplace for security, privacy, risk, and compliance experts. Through TalPoint, you can find the best compliance and cybersecurity experts. Plus, you will also save time and money because our cybersecurity hiring process will take care of all sourcing, vetting, selecting, and onboarding the best possible talent for your requirements!

→ Schedule a time to chat **to know how TalPoint can match you with the security consultant you need in just 48 hours.**

talpoint.com