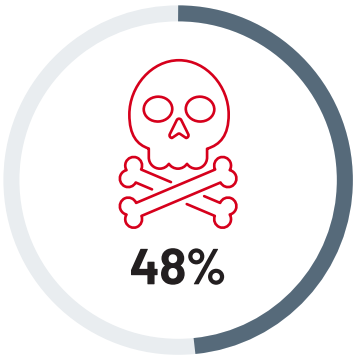
MANDIANT

MANAGED SERVICES
WHITE PAPER

Navigating the Cyber Skills Shortage



of organizations surveyed were a victim of at least one successful ransomware attack[1]

$10.5 trillion by 2025

estimated annual cost of cyber crime to companies[2]

$3.5 million

projected global workforce gap through 2025[6]

Introduction

It is predicted that the global cost of ransomware damage will exceed $265 billion by 2031[2] and some security researchers have estimated that cyber crime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015.[3]

These levels of threat activity prompt the demand for skilled workers, driving unprecedented employment activity—so much so that the global unemployment level for cyber security is at 0%.[4] This level of unemployment isn't going unnoticed, with 57% of organizations saying they have been impacted by the cyber security skills shortage.[5] With the projected global workforce gap at a staggering 3.5 million, which is expected to remain through 2025,[6] over 500,000 unfilled cyber security jobs in the US alone,[7] organizations are faced with a daunting task to recruit, hire and retain cyber security professionals.

Positive measures are being taken, but it will take years of focused effort to get the situation under control. In the meantime, organizations will need to review both long- and short- term strategies to securely navigate their way around the skills gap. This may well involve accepting a little short-term pain while long-term solutions are bedding in.

This white paper assesses and analyzes how the cyber security workforce gap may be affecting businesses and their employees and discusses a number of strategies which can be deployed to mitigate the risk of a successful attack.

1 ESG (November 30, 2021). ESG Research Report: 2022 Technology Spending Intentions Survey.
2 Cyber Crime Magazine (June 3, 2021). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031.
3 ESG and ISSA (July 2021). The Life and Times of Cybersecurity Professionals 2021, Volume V.
4 Security Intelligence (August 20, 2020). Your Newest Cybersecurity Professional Is Already in Your Company.
5 ESG and ISSA (July 2021). The Life and Times of Cybersecurity Professionals 2021, Volume V.
6 Ibid.
7 Cyberseek (2022). Cybersecurity Supply/Demand Heat Map.

The Cyber Security Workforce Shortage

There is a prevalent human factor to the success of cyber security; behind the technology lies a team of professionals with a range of technical skills used to implement defensive and proactive hunting strategies. While technology has a big part to play in the against cyber attacks, it is the human element which is both the catalyst for attack and defense.

Commercial realities

Historically, organizations viewed technology as the answer to cyber security. Buying the latest antivirus software led many to believe that sensitive data was protected from criminal activity. Today's truth is quite different. Threat actors work around the clock to break through security systems and even with compliance software, businesses remain at risk. Trained cyber security analysts must supplement cyber security software that is enabled to receive and interpret data to react to and report on the alerts and events.

Professionals in the cyber security industry are constantly playing catch-up with the threats they are defending against. Technology and criminal malice are developing fast enough to outpace the availability and skill level of new talent.

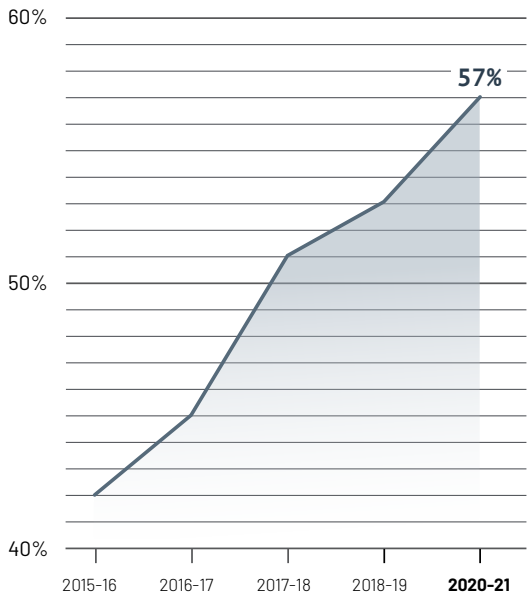


FIGURE 1. The percentage of organizations reporting a problematic shortage of cyber security skills.[11]

Given the range of capabilities needed for cyber security, no single expert will have all the skills needed to ensure a company's defense. Businesses need support from a wide range of security practitioners, including threat hunting analysts, intelligence analysts, malware reverse engineers, attack simulation specialists, incident responders and security program analysts. Against these needs, the growing workforce gap makes cyber security increasingly difficult.

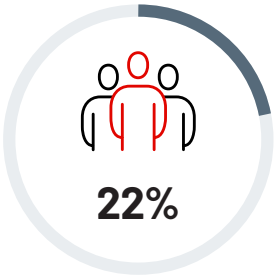
The impact of the skills gap on the global public and private sectors include increased burn-out among cyber security professionals, difficulty retaining talent, and the increased likelihood of breaches. Not all attacks will be successful but inadequately staffed organizations may be unable to cope with attack volume or sophistication.

The staffing economy

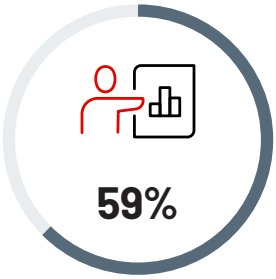
The limited cyber skills supply is driving the average salary of a cyber security worker up to a level many companies cannot accommodate. The public sector is particularly hard hit as their workers, heavily targeted by recruiters, migrate to the better-paid private sector. Seventy percent of cyber security professionals surveyed admitted to being solicited by a recruiter at least once per month.[8] If you combine that with the 76% that rated the difficulty of hiring and retaining skilled personnel as moderately high to high,[9] a carefully built team can quickly be lost to attrition or take a long time to rebuild.

The most difficult levels to hire are at the mid-career (4-7 years of experience) and senior career (7+ years of experience)[10]—those who have deeper knowledge and well-honed skills. Human resources teams are having to adopt faster and more efficient hiring processes and broaden candidate qualifications. As a result, many businesses are having to hire and train junior employees rather than hire people with the desired level of cyber security skills.

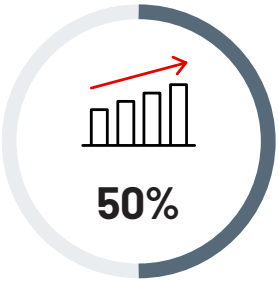
8 ESG and ISSA (July 2021). The Life and Times of Cybersecurity Professionals 2021, Volume V.
9 Ibid.
10 Ibid.
11 Ibid.



of cyber security professionals agree **it is hard to keep up with cyber security skills** given the demands of their job[12]



of **organizations are not providing an adequate level of training** for professionals in the sector[13]



of cyber security professionals say **job stress levels increased in past year** as a result of remote worker support due to Covid[14]

Professional stressors

A large paycheck may not always compensate an employee for high workplace pressures. Understaffed and underqualified security teams may spend a disproportionate amount of time on high-priority issues and incident response, with limited time left for planning, strategy and ongoing training.

If employees don't have time to refresh their skills or training budgets are not in place to facilitate learning, blame for an attack may be unfairly attributed to the cyber security team. The consequences include a drop in job satisfaction, high burn-out rate or migration of workers out of the sector.

Learning and adaptation are critical

Because the rules of engagement are continuously evolving, cyber security employees have to constantly update their knowledge on new attack methods to protect their employers, and those employers don't always provide training.

This lack of learning and knowledge sharing remains the most common contributor to security incidents.[15] Without training, professionals will be challenged to outmaneuver attackers. A recent survey by ESG indicated that 33% of cyber security professionals said they were unable to use some of their existing security technologies to their full potential,[16] indicating they may not only lack time to maximize functionality but also lack the ability to use and integrate those tools into their systems.

A circular dilemma

It is difficult to break this cycle. Employers are struggling to find and retain qualified staff. Qualified staff are overstretched, but still need investment from their employers to update their knowledge and skills.

When an employer recruits underqualified staff, existing workers are not only overworked to bridge the gap, but new employees must learn quickly and apply their newly acquired knowledge at an unrealistic pace. This can put additional pressure on teams.

12 ESG and ISSA (July 2021). The Life and Times of Cybersecurity Professionals 2021, Volume V.
13 Ibid.
14 Ibid.
15 Usecure (April 2019). The Role of Human Error in Successful Cyber Security Breaches.
16 ESG and ISSA (July 2021). The Life and Times of Cybersecurity Professionals 2021, Volume V.

Options for Bridging the Gap

Long-Term options

Businesses of all sizes can take steps to mitigate their risk including training, changing recruitment processes, machine learning or outsourcing specialized roles.

Expertise versus experience for risk mitigation

One possible way to resolve the skills gap is for organizations to develop an in-depth cyber security program in conjunction with experts and combine real-world exercises with actionable threat intelligence. Organizations can also continually provide resources that help team members stay up-to-date with attack trends. This sort of investment in existing staff, coupled with strong retention strategies, can be cost effective in the long term.

Security training and apprenticeships can be offered to a wide range of employees, from junior staff and recently hired college graduates to existing staff with the skills to adapt to a security role. A passionate and dedicated employee is not only going to be a great student, but with a fully immersive training and development program, they can become an even greater asset to the organization

To target and develop needed skills, organizations must assess their needs before developing or deploying a curriculum. A clear plan for mentoring, apprenticeships and accredited programs that include a repeatable process as new employees are introduced can change the fortunes of a company facing the skills crisis.

Training is a versatile solution applicable to businesses of all sizes. But during training, businesses still need to be protected from attack. Joining forces with an external partner may deliver the needed short-term value, especially if the partner can provide staff mentoring. Larger firms may also find some machine learning tools useful.

Adapting the recruitment process for hiring cyber professionals

High demand for cyber professionals means HR teams must revisit both their search criteria and recruitment methodology. Small tweaks to strategy and attitude can uncover a latent workforce. To hire skilled, trained staff, recruitment processes need to become more responsive and proactive. Numerous lengthy interview stages need to be replaced with dynamic, instinctive procedures which facilitate quick decisions leading to prompt offers of employment. Organizations that adapt more quickly are likely to have access to more qualified candidates.

If an organization has the the ability to train newly hired staff through apprenticeships, mentoring or a certified course, HR teams need to expand their search criteria to identify broader and stronger applicant pools. Universities and higher education providers are a natural place to start, especially when it comes to apprenticeships. Many businesses also look to military veterans transitioning to civilian life. Military personnel have exposure to the latest IT tools, implementing good security practices and protocols comes as second nature to them.

Opportunities to support diversity in the industry can also provide the potential to improve the skills gap. There is opportunity to increase the number of female professionals in the cyber security sector, which currently stands at 25%.[17]

Workable, proactive solutions that deal with recruitment can be broadly applied to any size organization. Methods used may vary depending on budget and resources, but the underlying strategy and approach is the common denominator across all businesses.

17 Cybersecurity Ventures (November 9, 2021). Cyber Security Jobs Report: 3.5 Million Openings in 2025.

Long-Term options

Development of an automated workforce

Machine learning or automated processes can be used to help both less experienced teams and larger organizations evaluate threats or process large amounts of data.

There are different views of the role machine learning and automation will play in the security arena in the future. For now, while automated procesesses` may be able to predict and sense the early stages of attack and even contain it, attackers will be constantly working to subvert and work around it.

> It is unlikely that machine learning will ever truly replace a skilled team, but it can help automate mundane, repetitive tasks.

Incorporating machine learning into a business allows security teams to focus their attention on strategic planning, assessment and real- time threat response and analysis to protect organizations more effectively.

Outsourcing cyber security

Managed security service providers (MSSPs) and more specialized managed detection and response providers can help boost or fulfill the responsibilities of in-house cyber security teams. Delivering a wide variety of services from across endpoint, network, cloud, email and operational technology to surface impactful events and leverage proven response tactics they are designed to reduce overall overhead while giving access to specialized professionals.

As the services market for cyber security matures, it is changing shape. MSSP offerings are becoming more dynamic. Leveraging security products and operational services with frontline intelligence is now becoming more commonplace, helping businesses get the most out of security solutions while simultaneously improving their in-house skills.

Flexibility to close the skills gap

Because of the cyber skills gap, many organizations struggle to achieve full cyber security maturity. Organizations need the flexibility to engage with security experts —based on their immediate needs or longer term projects. This could include outsourcing cyber security completely, creating a custom engagement to create a security strategy, to on-demand access to experts to address questions or create comprehensive or individual training plan for employees.

Conclusion

The nature and severity of the cyber security skills shortage has been fostering debate throughout social media, industry bodies and businesses for some time now.

There are very few industries today which face a constantly evolving and increasing threat landscape in the way that cyber security does; as such, there is no "one-size-fits-all" solution simply because professionals, along with the aid of technology, are still getting to grips with the situation.

There are a number of near- and longer-term options to mitigate the risk of a security breach available to businesses of all sizes, with staff training being the most prevalent. Whether training new employees who are looking to build on their skills, or updating knowledge within existing teams, training has time and again been identified as a reliable method for improving the skills gap issue. Training is accessible to all organizations and is also an effective method to retain teams at a time when mounting work pressures and aggressive head-hunting techniques are at their peak.

For midsize to large enterprises, frontline intelligence and support delivered by MSSPs can be the preferred route, with many providers responding rapidly to the market, creating desirable services which simultaneously protect and coach clients.

The right mix of solutions and flexible access can only be determined by each individual business; their needs, perceived exposure to risk and of course, budgets. To succeed, organizations must be cognizant of the risks and rewards generated by the solutions currently available, both in the short- and long-term.

Learn more at **www.mandiant.com**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT®
YOUR CYBERSECURITY ADVANTAGE