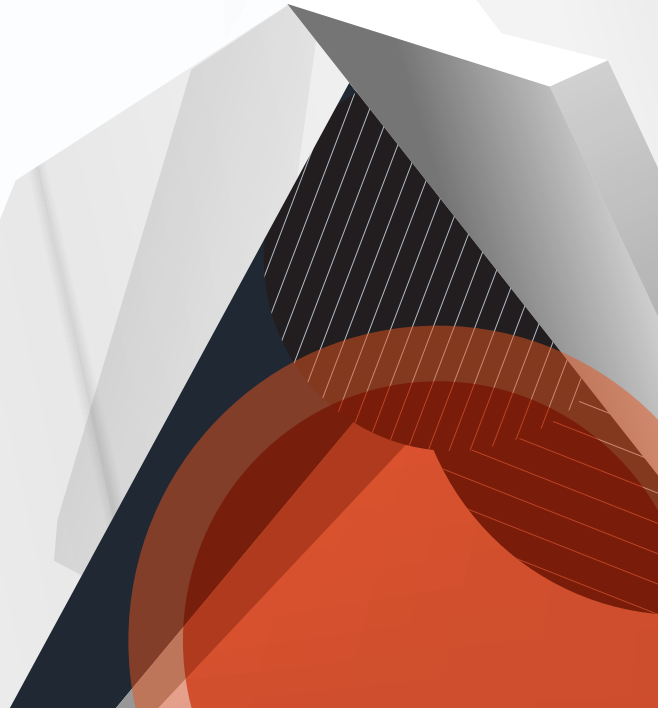
FIREEYE™

WHITE PAPER

Combat the Cyber Skills Shortage



ONE

of organizations surveyed experienced at least one successful cyber attack in 2018

$2.1 trillion
is the estimated total cost of cyber crime in 2019

3.5 million
is the projected global workforce gap for 2022

Introduction

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

Cyber attacks have risen to such a level that in 2018, 77% of organizations surveyed had borne the brunt of a successful attack at least once in the last 12 months.[1] Although worldwide spending on information security has been predicted to grow to $124 billion, some security researchers have estimated the total cost of cyber crime will quadruple in 2019 to $2.1 trillion, outpacing cyber security spend by 16 times.[2]

These levels of threat activity prompt the demand for skilled workers, driving unprecedented employment activity in a sector which is still relatively new—so much so that the global unemployment level for cyber security is yet to exceed 2% (1% in Europe). In 2018-19, 53% of organizations said they felt there was a problematic shortage of cyber security skills[3] (up 11% on 2015). The projected global workforce gap for 2022 is a staggering 3.5 million.[4]

Positive measures are being taken, but it will take several 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] CyberEdge Group, LLC (2018). 2018 Cyberthreat Defense Report. https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf
[2] Gartner (August 15, 2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
[3] ESG, ISSA (April 2019). Life of Cybersecurity Professionals
[4] Frost & Sullivan (2017). Global Information Security Workforce Study, Benchmarking Workforce Capacity & Response to Cyber Risk.

The Cyber Security Workforce Shortage

Commercial Realities

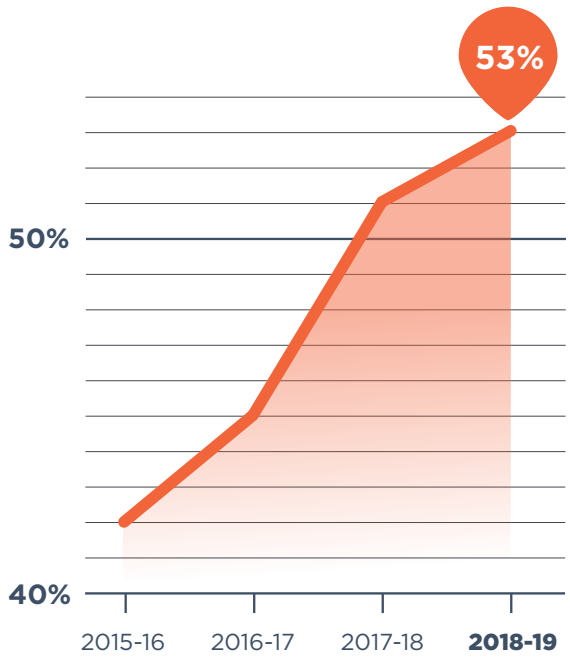
Historically, organizations viewed technology as the answer to cyber security. Buying the latest antivirus software led many to believe that sensitive data was protected from criminal activity. Today's truth is quite different. Hackers work around the clock to break through commercial security software and compliance software still leaves businesses at risk. Trained staff are required to supplement cyber security software that is supposed to receive data, interpret, react to and report on 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 so quickly, they are outpacing the availability and skill level of new talent.

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.[5] 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.

Figure 1: The percentage of organizations reporting a problematic shortage of cyber security skills



The Staffing Economy

The limited cyber skills supply is driving up the average salary of a cyber security worker 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. Forty-four percent of cyber security professionals surveyed admitted to being solicited by a recruiter at least once a week to consider other cyber security jobs,[6] which means a carefully built team can quickly be lost to attrition. In a 2019 study by IBM, only 30% of respondents reported having sufficient cyber security staff and 75% rated the difficulty of hiring and retaining skilled personnel as moderately high to high.[7]

The most pressing skills shortage lies at the junior to mid-management level—those who perform operational and tactical security work. 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 appropriate level of cyber security skills.

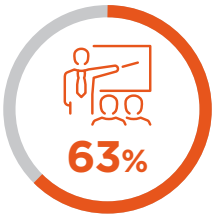
Figure 1: ESG, ISSA (April 2019). Life of Cybersecurity Professionals

[5] FireEye How to Enhance Your Security Team *https://content.fireeye.com/expertise-on-demand/eb-expertise-on-demand.*

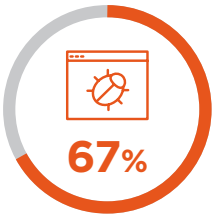
[6] ESG, ISSA (2018). The Life and Times of Cybersecurity Professionals.

[7] IBM Security (April 11 2019). Study on the Cyber Resilient Organization.

of cyber security professionals agree it is hard to keep up with cyber security skills given the demands of their job[8]



of organizations are not providing an adequate level of training for professionals in the sector[9]



of respondents said they do not have the time or the resources to mitigate every bug[10]

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. Not surprisingly, only 39% of employees in the cyber security sector recorded that they were very satisfied in their job.[11]

The negative morale generated from the staffing crisis can be an additional stressor for new and emerging cyber professionals.

Learning and Adaptation are Critical

Unlike many industries, cyber security 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 has been the most common contributor to security incidents.[12] Without training, professionals will be challenged to outmaneuver attackers. A recent survey by ESG indicated that 47% of cyber security professionals said they were unable to use some of their existing security technologies to their full potential,[13] 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 unqualified 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.

---

[8] ESG, ISSA (2018). The Life and Times of Cybersecurity Professionals.
[9] ESG, ISSA (2018). The Life and Times of Cybersecurity Professionals.
[10] C.Osborne (February 2 2019). One In Three Enterprises Can't Protect Themselves From Data Breaches. https://www.zdnet.com/article/one-in-three-enterprises-cant-avoid-data-breaches/
[11] ESG, ISSA (November 2017). The Life and Times of Cybersecurity Professionals.
[12] ESG, ISSA (November 2017). The Life and Times of Cybersecurity Professionals.
[13] ESG, ISSA (November 2017). The Life and Times of Cybersecurity Professionals.

Options for Bridging the Gap

LONG-TERM OPTIONS

Businesses of all sizes can take steps to mitigate their risk including; training, changing recruitment processes, Artificial Intelligence 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 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 Artificial Intelligence (AI) solutions useful.

Adapting the Recruitment Process

Due to the competition for cyber professionals, HR teams need to 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 is willing 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 11%.[14] A recent study showed that women in the cyber security profession enter the industry with higher education levels than men, but 51% of female security professionals surveyed responded that they experienced various forms of discrimination,[15] reducing their motivation to stay in the sector.

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.

[14] Frost & Sullivan (2017). The 2017 Global Information Security Workforce Study: Women In Cybersecurity.
[15] Frost & Sullivan (2017). The 2017 Global Information Security Workforce Study: Women In Cybersecurity.

NEAR-TERM OPTIONS

Development of an Automated Workforce

Even in its early stages, the potential of AI is obvious. It can be used to help inexperienced teams evaluate threats or process large amounts of data.

There are two views of AI in the security arena. The first is that security teams may struggle to adopt and operate it without further training. The second is that AI may be capable of replacing a security team entirely. This latter view seems unrealistic. While security AI 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 AI will never truly replace a living, breathing team, but it can automate mundane, repetitive tasks.

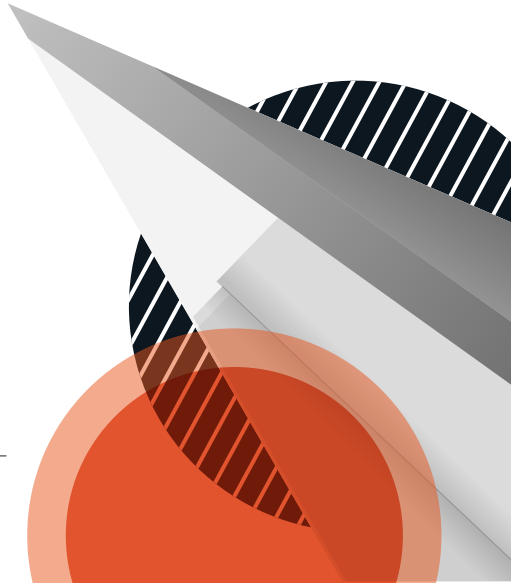
Incorporating AI into a business allows security teams to focus their attention on strategic planning, assessment and real-time threat response and analysis to more effectively protect organizations. AI may not be for everyone, but for some it may be invaluable.

Outsourcing Cyber Security

Managed security service providers (MSSPs) can provide an immediate boost to or fulfill the responsibilities of in-house cyber security teams. Delivering a wide variety of services from firewalls, intrusion detection, virtual private networks, vulnerability scanning and antivirus services, they are designed to reduce overall overhead while giving access to specialized professionals. Nearly nine in 10 companies surveyed are turning to external experts to help support their business.[16]

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

The number of MSSPs in the market is growing rapidly, due in part to disillusioned and burnt-out security professionals opting for a more lucrative employment path.



[16] CyberEdge Group, LLC (2017). 2017 Cyberthreat Defense Report. *https://cyber-edge.com/wp-content/uploads/2017/03/CyberEdge-2017-CDR-report.pdf*

Conclusion

The nature and severity of the cyber security skills crisis 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 destructive 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 have the will to work but lack necessary skills, or updating knowledge within existing teams, training has time and again been identified as the number one method for improving the skills gap issue. Training is accessible to both smaller and larger 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 is a preferred route, with many providers responding rapidly to the market, creating desirable services which simultaneously protect and coach clients.

The right mix of solutions 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.

To learn more about FireEye Expertise On Demand, visit: **www.FireEye.com/Expertise**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™