Understanding the Cybersecurity Skills Gap: The Expert View

The skills gap is one of the most debated, enduring, and pressing issues in the cybersecurity world. While awareness of cybersecurity as a lucrative and rewarding career path has improved significantly in recent years, rapid technological advances have kept the skills gap alarmingly wide.

Generative AI models have supercharged attack rates, threat actors are growing more sophisticated by the day, and defensive technologies are evolving at unprecedented speed, meaning the industry is pushed harder than ever to close the gap and keep attackers at bay.

Same Problem, Different Day

Closing the cybersecurity skills gap is a persistent problem, but one that has changed with time. In previous years, the industry was focused on getting more people trained and into cybersecurity roles.

Today, the more pressing issue is upskilling existing cybersecurity professionals to keep up with emerging threats and technologies. Moreover, recent research has driven home the importance of diversity, inclusivity, and accessibility in closing the cybersecurity gap, and the need for improved soft skills has become increasingly apparent.

These nuances make for an incredibly complex problem, but not an insurmountable one. The cybersecurity industry is full of talented, thoughtful, and creative individuals who solve complex problems for a living. We decided to start tackling those fundamental issues - what causes the cybersecurity skills gap, why it matters, and how we can fix it - by talking to some of those experts. Here are their thoughts.

Kirsten Doyle

Cybersecurity Content Writer

LinkedIn

1). Is there a skills gap in the cybersecurity industry?

Yes, there is a dire shortage of cybersecurity skills across various domains, thanks to the evolving nature of cyber threats and the rapid advancement of technology. Malicious actors are growing increasingly cunning and determined and are constantly honing their Tools, Techniques, and Procedures (TTPs). Cybersecurity professionals are always on the back foot, which means the development of skilled professionals needs to catch up with the demand. Unfortunately, this skills gap leaves businesses across the public and private sectors vulnerable to attack. Defense mechanisms are rendered vulnerable to modern, complex threats without the necessary skills.

I think it's important to note that it's not only finding these skills that's a problem; it's hanging on to them, too. The rapid technological advancements mentioned mean continuous learning and training are needed, putting overstretched professionals under more pressure to stay updated. The evolving nature of cyber threats means constant adaptation, which can lead to skill obsolescence if not regularly updated. Moreover, understanding the rarity of highly experienced professionals, large enterprises with huge budgets can afford lucrative salaries to tempt these individuals to pursue higher-paying positions elsewhere. In addition, burnout is a real problem in such a high-pressure field, further adding to skill turnover.

2). Is the gap only in certain areas within the cybersecurity industry?

While there is a general skills deficit, I have noticed it particularly in programming knowledge, cybersecurity operations, penetration testing, threat analysis, and cloud security. When it comes to programming knowledge, the shortage stems from the increasing complexity of software and the demand for secure coding practices. Many developers lack sufficient training in secure coding principles, leaving software vulnerable to exploitation.

Cybersecurity operations are a problem because businesses are battling to find skilled people capable of managing and maintaining security infrastructure - a wide variety of skills are needed. This includes monitoring systems for anomalous activities, responding to incidents immediately, and implementing effective security measures. There are also many different views on cybersecurity and what constitutes robust, proactive defense - it's a broad discipline.

Penetration testing is another area that is short on skills. To do this effectively requires individuals with expertise in identifying and exploiting vulnerabilities within systems and networks. This is an incredibly technical area that needs deep technical knowledge as well as ethical hacking skills.

Similarly, threat analysis needs those capable of understanding and predicting cyber threats, which is no simple feat in such a rapidly evolving landscape. Few people have the expertise to analyze emerging threats and develop effective security strategies. Finally, cloud security is in high demand in a world of distributed workforces and as more companies transition to cloud-based environments. There simply aren't enough professionals with the necessary expertise in securing cloud infrastructures and applications. Also, applications built for on-prem don't necessarily work well in the cloud and can lead to all sorts of security issues if not migrated properly.

It's also worth mentioning that softer skills, such as communication, critical thinking, problem-solving, attention to detail, among others, are also needed.

3). Is it possible to eliminate the skills gap? If not, what can be done to make progress in closing the skills gap?

I don't believe, at this stage, it's possible to eliminate it altogether. Having said that, businesses play a crucial role in addressing the skills gap by continuously training their workforce. Regular skill updates are non-negotiable to fight evolving cyber threats successfully. By introducing internship and mentorship programs, businesses can open up opportunities for learners looking to explore this field and perhaps make a career for themselves. Similarly, collaborating with educational bodies involved in upskilling and reskilling programs helps attract and retain digital professionals.

Of course, creating a more diverse and inclusive cyber workforce is also essential for developing cybersecurity skills. Removing hiring barriers and providing accessible resources and training programs to people of all sexes, ages, and cultures will go a long way toward addressing the skills shortage.

This also needs to be a collective effort - closing the cybersecurity skills gap requires collaboration and commitment from all stakeholders.

Ali Haider

Senior Cybersecurity Consultant

LinkedIn

1). Is there a skills gap in the cybersecurity industry?

The cybersecurity industry confronts a significant skills gap driven by the constant evolution of cyber threats, escalating demand for skilled professionals, and deficiencies in traditional educational pathways. This gap is exacerbated by challenges in retaining talent and fostering diversity. Addressing this disparity necessitates substantial investments in education and training programs tailored to cybersecurity, ensuring the cultivation of a capable workforce. Promoting diversity and inclusivity within the field, fostering collaboration between academic institutions and industry stakeholders, and implementing initiatives for upskilling and reskilling are vital components of the solution. By adopting a multifaceted approach that spans education, recruitment, and retention efforts, organizations can mitigate the shortage of cybersecurity talent and fortify their defenses against increasingly sophisticated cyber threats. Closing the skills gap is paramount in safeguarding digital assets and maintaining resilience in the face of evolving cyber risks.

2). Is the gap only in certain areas within the cybersecurity industry?

While the skills gap is a widespread issue across the cybersecurity industry, it may manifest more prominently in certain specialized areas. These areas often require highly technical skills and deep domain expertise, making it challenging to find qualified professionals. Some examples of specialized areas where the skills gap may be particularly pronounced include:

- Incident Response and Forensics: Professionals in this area need to have a deep understanding of cybersecurity incidents, including the ability to investigate breaches, analyze evidence, and develop response strategies.

- Threat Intelligence Analysis: Analysts in this field must possess advanced knowledge of threat actors, Tactics, Techniques, and Procedures (TTPs) to identify and mitigate emerging cyber threats effectively.

- Cryptography and Encryption: Experts in cryptography play a crucial role in designing and implementing secure cryptographic algorithms and protocols to protect sensitive data and communications.

- Cloud Security: With the increasing adoption of cloud computing, there is a growing demand for professionals skilled in securing cloud environments, including knowledge of cloud architecture, configuration management, and cloud-specific security tools.

- IoT Security: As the Internet of Things (IoT) continues to expand, there is a need for professionals who understand the unique security challenges posed by interconnected devices and can implement effective security measures to mitigate risks.

- Industrial Control Systems (ICS) Security: Professionals in this area focus on securing critical infrastructure, such as power plants and manufacturing facilities, from cyber threats that could have significant real-world consequences.

While the skills gap exists across the cybersecurity industry, addressing it may require targeted efforts to develop talent in these specialized areas where demand is particularly high, and the pool of qualified professionals may be limited.

3). Is it possible to eliminate the skills gap? If not, what can be done to make progress in closing the skills gap?

Completely eliminating the skills gap in the cybersecurity industry may be challenging due to the ever-evolving nature of cyber threats and technologies. However, significant progress can be made in closing the gap through a combination of strategic initiatives:

- Comprehensive Education and Training: Investing in robust cybersecurity education and training programs at all levels, from K-12 to higher education and professional certifications, can help develop a pipeline of skilled professionals with up-to-date knowledge and expertise.

- Industry-Academia Collaboration: Facilitating collaboration between academic institutions and industry partners can ensure that educational programs are aligned with the current and future needs of the cybersecurity workforce. This collaboration can include curriculum development, guest lectures, internships, and research partnerships.

- Upskilling and Reskilling: Providing opportunities for current professionals to upskill or reskill through training programs, workshops, and certification courses can help bridge the skills gap and adapt to emerging technologies and threats.

- Diversity and Inclusion Initiatives: Promoting diversity and inclusion within the cybersecurity field can broaden the talent pool and bring in fresh perspectives and innovative solutions. Initiatives such as scholarships, mentorship programs, and outreach efforts to underrepresented groups can help diversify the workforce.

- Continuous Learning and Professional Development: Encouraging a culture of continuous learning and professional development within organizations can ensure that cybersecurity professionals stay abreast of the latest trends, technologies, and best practices in the field.

- Government and Industry Collaboration: Governments, industry associations, and professional organizations can collaborate to address the skills gap through initiatives such as workforce development grants, tax incentives for training programs, and information-sharing networks.

While completely eliminating the skills gap may be unrealistic, these proactive measures can make significant progress in closing the gap and ensuring that organizations have the skilled cybersecurity professionals they need to protect against evolving threats.

Anastasios Arampatzis

Cybersecurity Content Writer

LinkedIn

1). Is there a skills gap in the cybersecurity industry?

Emphatically yes. Cybersecurity is a rapidly evolving field, with new threats and technologies emerging constantly. This gap is fueled by a constant cat-and-mouse game between cybersecurity professionals and evolving technology-enabled risks. As technology advances, malicious actors develop sophisticated tools and techniques to exploit vulnerabilities. Cybersecurity professionals must constantly adapt and learn new skills to stay ahead, making it a true challenge to find qualified talent. This mismatch creates a significant business risk for organizations across the globe, which is highlighted year after year by various reports such as the World Economic Forum Global Risks Report.

2). Is the gap only in certain areas within the cybersecurity industry?

The skills gap extends beyond technical domains. We face a pronounced soft skills gap – skills like communication, problem-solving, empathy, and kindness. These are critical in a sector often dominated by Fear, Uncertainty, and Doubt (FUD). Effective communication skills help translate complex threats into actionable insights for non-technical audiences. Problem-solving is essential for devising innovative solutions in a crisis. Empathy and kindness lay the groundwork for the trust and collaboration needed to strengthen an organization's overall cyber resilience. Tackling this softer side of the skills gap is a complex challenge but vital for the health and effectiveness of the industry.

3). Is it possible to eliminate the skills gap? If not, what can be done to make progress in closing the skills gap?

While complete elimination of the gap is improbable given the dynamic nature of cybersecurity, we can significantly narrow it by focusing on several key strategies:

- Prioritize the human element: Invest in your existing workforce. Provide opportunities for reskilling and upskilling, empowering them to keep pace with evolving threats.

- Hire for potential: Look for aptitude, problem-solving skills, and adaptability rather than fixating solely on traditional degrees.

- Foster early interest: Partner with educational institutions to spark a passion for cybersecurity. Curriculum reforms like introducing robotics in early education can nurture a future pipeline of talent.

Finally, it's crucial to ask ourselves: are we learning from our past mistakes before diving into new technologies? Should we pause, reflect on our achievements, and critically evaluate the future trajectory of our technological landscape?

Dr Jessica Barker MBE

Author of 'Hacked: The Secrets Behind Cyber Attacks' and 'Confident Cyber Security: The Essential Insights and How to Protect from Threats'

Linkedin

1). Is there a skills gap in the cybersecurity industry?

I know lots of people - great people - searching for their next opportunity in cyber security. I hear from people every week, often readers of Confident Cyber Security, who are so keen to get into this field. I know some really skilled, experienced people who have been laid off. I also know lots of people who are hiring, who are struggling to hire, and who can't find the right people for the vacancies that they have. In the cybersecurity community, we've been talking about this for years but are making little progress in bridging the gap. My impression has long been that the majority of job vacancies don't match the type of roles that job seekers are looking for, that there aren't enough entry-level jobs available, and that many teams are too busy and under too much pressure to train new starters in cyber security.

This leads to greater burnout for individuals and teams within the field, deep frustration for many of those looking or their first or next opportunity, and greater cyber security risk for organizations.

Specializing in cybersecurity awareness, I know that behavior and culture come with some unique frustrations. About eight years ago – when I was already five years into my work in this area - I remember seriously considering retraining as a pentester because there were so few opportunities to work with companies on the human side of cyber security. Then, things started to change. Cyber security awareness, behavior, and culture moved up the agenda and into more mainstream conversations. Now, most security leaders and teams understand the importance of people in security to at least some degree, and many recognize that getting the people part of the equation right is the most important element. However, budgets and job opportunities still do not match this apparent understanding.

Yiannis Kanellopoulos

Founder & Chief Executive Officer of Code4thought

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

Companies should indeed be deeply concerned about the skills gap within the cybersecurity industry. Similar to the broader IT sector, where demand consistently outpaces supply, the cybersecurity realm faces a shortage of qualified professionals. This discrepancy is exacerbated by the escalating volume, diversity, and intricacy of cyber threats, which necessitate a commensurate increase in skilled talent to safeguard organizational digital assets. Failure to address this gap leaves companies exposed to a plethora of risks, including data breaches, financial losses, reputational damage, and legal ramifications. If we also take into account the fact that currently, digitalization pervades every aspect of business operations, the consequences of inadequate cybersecurity measures can be grave, potentially undermining trust with customers and stakeholders and impeding business continuity.

2). Is it a technical skills gap, a soft skills gap, or both?

The skills gap in cybersecurity encompasses both technical expertise and soft skills, although the latter may present a more serious challenge. While acquiring proficiency in the technical aspects of cybersecurity is undeniably critical, mastering soft skills is equally indispensable. Effective communication, problem-solving, critical thinking, and teamwork are paramount, particularly as many cyber threats exploit human vulnerabilities or employ sophisticated social engineering tactics. As such, the ability to collaborate seamlessly within cross-functional teams, articulate complex concepts to diverse stakeholders, and adapt swiftly to evolving threats is pivotal for success in combating cybercrime. Therefore, while technical proficiency serves as the foundation, it is the integration of soft skills that enables cybersecurity professionals to navigate the intricacies of their roles adeptly and mitigate risks effectively.

3). Does the skills gap lead to greater cybersecurity risk?

Unquestionably, the skills gap in cybersecurity poses a substantial risk to organizations, amplifying their vulnerability to cyber threats. With a shortage of skilled professionals to counter the mounting number and sophistication of attacks, companies find themselves ill-equipped to defend against evolving cyber risks. This deficiency undermines their ability to detect, prevent, and respond to threats in a timely and effective manner, heightening the likelihood of successful breaches and their attendant consequences.

Moreover, the absence of proficient cybersecurity practitioners impedes the implementation of robust security measures and best practices, leaving organizational systems and sensitive data exposed to exploitation by malicious actors. However, it is imperative to recognize that the cybersecurity industry can leverage technological advancements to mitigate the impact of the skills gap. By investing in automation, artificial intelligence, and machine learning technologies, organizations can augment their cyber defense capabilities, bolster resilience, and alleviate the burden on talent resources. Thus, while the skills gap presents serious challenges, proactive adoption of innovative solutions can mitigate its adverse effects and enhance the overall cybersecurity posture.

Ross Moore

Cybersecurity Analyst

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

Companies should be primarily concerned about the gap in their own company first. It's easy to get carried away by statistics and reports. It's important to take stock of what one's organization needs.

One way stats are useful is by bringing forth the potential lack of security in your vendors. This can be alleviated by having an applicable vendor/third-party risk assessment process. It protects one's own company but also helps drive the industry when many customers ask for security assurance. That security requirement by prospects makes cybersecurity become a business driver for vendors, and it becomes viewed more as an investment instead of an expense. This requires vendors to hire the appropriate security personnel.

2). Is it a technical skills gap, soft skills gap, or both?

According to various reports over the last few years, there's approximately a 75% skills gap worldwide. The largest apparent gap is in relevant technical skills - especially in engineering and architecture - whereas in leadership skills, there's appropriate coverage overall.

Yes, there's a soft skills gap, but soft skills are a challenge in any industry and company, so it's not a challenge relegated to cybersecurity. Why is it such a challenge? Likely because of a hyperfocus of so many industries interacting with computers instead of interacting with people.

When addressing the gaps, the well-known model of People, Processes, Technology (PPT) is a good cycle to follow. People first - it's all about people first and foremost. Web development, products and services, sales, security - it's first and last about people - providing good products and services and securing everyone's digital assets. When the People puzzle piece is in place, then Processes and Technology can be figured out. And it's an iterative – even non-linear – cycle. One affects the other. But putting either of the other two before People creates major business issues.

3). Does the skills gap lead to greater cybersecurity risk?

Definitely. Organizations need to ask:

1: What are my gaps?

2: How am I going about filling those gaps?

#1 is about getting away from statistics and looking closely at one's own needs. If you can't answer #1, then #2 won't happen, either. Like in marketing, you need to know your target audience. In this case, the personnel needed. Who are you looking for to fill the gaps?

The honest answer may be: "I have no clue!" And that's a fine answer. Businesses are in the business of risk - all businesses operate on some level of risk, and all along the way, they encounter financial, reputational, product, service, and many other risks. And they do something about it. They have meetings, hire consultants, and spend money on market research, all so they can figure out their business strategy and make proper decisions.

But there's often some kind of block with the word "security" that freezes up so much potential. Suddenly, it's too time-consuming, expensive, or resource-intensive to find out.

Security is now part of the foundation of business (along with Privacy) - more and more businesses like to see SOC 2, ISO 27001, or some other relevant cybersecurity attestation. Also, cybersecurity means different things to different people - sometimes it's highly technical, sometimes it includes Governance, risk management, and Compliance (GRC), and sometimes it's more like network/sysadmin duties. A company might simply need someone who has a penchant for technology and attention to detail to manage access control, set up some alerts, configure the firewall, and perform other foundational duties, but the job requirements somehow come across as needing someone who has three certifications, seven years of cloud experience, deep knowledge of Open Source Software (OSS), and programming expertise. Does the requisite position need a higher-level expert? Or do they need someone who is simply experienced and can grow into an expert? Determining the skills a company needs is incumbent on the individual company, and those individual determinations will work toward closing the overall skills gap.

Ian Thornton-Trump

Chief Information Security Officer

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

Out of all the things companies should be worried about, a skills gap in the cybersecurity industry is not one – that is a worry for government policymakers and the educational system. It's their job to make sure the economy has jobs in all sectors to sustain growth. If your country's gross domestic product (GDP) depends on knowledgeable workers and technical skills, it's up to the country's leadership to recognize those trends and plan accordingly, either with direct investment or attractive immigration policies for skilled workers. The only organizations that can deal with macro trends in society are the organizations that can make decisions at a macro level.

Companies should understand that they need to prepare their knowledge and IT skilled workers for change, providing training and support for their current and future needs. If the company treats knowledge workers and skilled tech workers as disposable commodities, then they should be worried that the "gap" will appear in their company and not their competition. Treat people fairly, provide supportive management, offer a competitive salary, and proactively prepare for future business needs. The skills gap will be a "someone else's company" problem.

2). Is it a technical skills gap, a soft skills gap, or both?

As new technology comes on board, the skill sets of the latest and greatest technology experts will react to the laws of supply and demand – that's the way the system works. Technical skills can be found in-house, assuming you were successful in re-skilling and upskilling those existing resources. If the technological investment has been characterized as continuously stacking on layers of tech and never addressing the technological debt, then the company is fairly doomed already, as it will have no capacity to take on new tech.

Tech skills can always be found in the market with a number of routes open - by paying a premium, finding an IT provider with the resources needed, exploring overseas outsourcing, or visa sponsorship opportunities, which are all options on the table. Magically thinking that new technological experts will suddenly appear in your own company without providing direction, training, a strategy, or a vision is folly and a basic failure of executive leadership.

When it comes to a soft skills gap, it exists. It's found with the demonstratable ridiculous and short-sighted practice of promoting tech workers to managerial levels without coaching, mentorship, and management training as part of that promotion package. Again, many companies have built their own nightmare scenarios and end up paying the price. A lead developer, promoted to CTO or System Architect, has a meltdown and leaves for new opportunities – the organization suffers the loss of both a great developer and the disruption of a high-level leadership departure. Again, leadership failure at the highest levels.

3). Does the skills gap lead to greater cybersecurity risk?

It's hard to reconcile the idea that a skills gap has any impact on cyber security business risk. It would be great if there was a tangible relationship where investment at the macro level yielded a demonstratable benefit; measurements are elusive. What we hear and see in the press is a collective view of post-breach analysis, which does not even get the basic security right when it comes to company security and does not even put in basic tooling and safeguards. This strikes me as a knowledge gap among non-cyber industry executive leadership and not an on-the-ground skills issue.

If non-cyber executives fully understood the company's risk posture when it came to cybersecurity, it would not be such a struggle to convince the organization to invest in basic cybersecurity – either it's not understood, or the message being sent by the cyber team is incoherent. All the skills in the world can't make up for underinvestment and hauling a junk pile of technological debt into the next decade – as time goes by, this tech mound becomes more vulnerable. It's heartbreaking to think that the state of cyber security falls onto the shoulders of the professionals who are doing the best they can with the technology they have. Perhaps the demoralizing "Velcro morale patch" for cyber security is "Expect to Self-Rescue. No one is Coming." Perhaps if executive leadership knew more about cyber risk, they would do more about cyber risk.

Jane Frankland

Chief Executive Officer of KnewStart & Founder of The IN-Security Movement

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

I believe they should be. Cyberattacks and data breaches are happening more frequently, and as businesses rely more and more on digital operations, the need for strong cybersecurity has never been higher. Unfortunately, there aren't enough skilled cybersecurity experts to protect the volume of organizations in need from these threats. According to the 2023 Workforce Study released by ISC2, the global cybersecurity workforce needs four million people, and a 12.6% increase from the previous year signifies a critical deficiency in the industry. This shortage poses not only operational challenges for businesses, leaving them wide open to attacks, data manipulation, and leaks, but it also raises significant concerns about the overall resilience of their cybersecurity defenses. It's a serious problem that needs immediate action from companies, policymakers, and schools to address the growing cybersecurity challenges.

2). Is it a technical skills gap, soft skills gap, or both?

In cyber, there's not just a lack of technical skills but also a shortage of essential soft skills like communication and leadership. This means that even though professionals may have the technical know-how, they might struggle with crucial abilities needed to deal effectively with cyber threats. I believe that, as an industry, we're now recognizing the importance of both technical expertise and soft skills in combating evolving challenges. Increasingly, I'm hearing of hiring managers who are looking for qualities beyond just technical knowledge, such as Artificial Intelligence understanding and teamwork capabilities, to bridge this gap. I find this encouraging as it highlights the pressing need for cybersecurity professionals to be not only tech-savvy, especially as cyber is a diverse and multi-disciplined field, but also adept at communication and adaptable in the face of cyber risks.

3). Does the skills gap lead to greater cybersecurity risk?

Yes, the skills gap in cyber can indeed lead to increased cybersecurity risks. When there is a shortage of professionals with both technical expertise and essential soft skills like communication and adaptability, organizations may struggle to effectively protect themselves against cyber threats. This lack of skilled professionals can result in vulnerabilities going unnoticed or unresolved, making it easier for cyber attackers to breach systems and steal sensitive data.

It also creates stress and burnout for existing security team members, which increases the likelihood of them leaving their current roles. Essentially, the skills gap creates a situation where organizations are less equipped to defend against cyber threats, ultimately heightening the overall cybersecurity risk they face.

Andra Zaharia

Cybersecurity Communication Manager

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

Whether they have cyber in their job title or not, there's no denying that the body of specialists doing cybersecurity work is sorely undersized compared to the task at hand. In my view, this has to do with human nature; our curiosity has simply always outweighed our cautiousness. This is why we continue to build technology with innovation as a driver, not security.

A legitimate cause for concern is not just the skills gap that keeps cybersecurity in catch-up mode but also its place in our culture. The perception that information security is a restraint on the exuberant pace of technology development lives on. Until we peel off this label, we might lose people who would do great work in cybersecurity to other disciplines and other roles.

And it's not just companies who need to pay attention to this area, but all of us - especially those of us who know about the responsibility cybersecurity carries and care about it.

2). Is it a technical skills gap, a soft skills gap, or both?

It's definitely both, in my view, and they fuel each other. To effectively communicate the growth prospects, engaging challenges, and rewards of working in cybersecurity is crucial. That's because it's key to attracting more people interested in developing the technical skills the work requires.

The better we can connect with people's needs and aspirations, the more willing they become to put in the work necessary to do meaningful cybersecurity work. We need to become vocal advocates for our own community to catch the eye of people who care about the same things we do. And then, we need to support them on their way to acquire the skills to both solve technical problems and the human challenges to which they're tied.

3). Does the skills gap lead to greater cybersecurity risk?

There can be a compound effect of the cybersecurity skills gap beyond what we're seeing right now. To estimate what it will take to meet future security challenges, we might look at medicine and see how this discipline has trained both generalist and specialized doctors to deal with the evolving nature of human health.

Cybersecurity being a multidisciplinary space, we can borrow even more approaches from other fields to enrich our ability to find and train the right people who understand risk and have a personal stake in reducing it. And skin in the game is particularly important in making cybersecurity a relevant and interesting development opportunity for Gen Z, whose energy and ingenuity we really need!

Panagiotis Soulos

Global Information Security Manager

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

Cybersecurity was, is, and will continue to be essential to organizations to protect their valuable assets. Due to the rapid and ongoing rise of technological advancements and the easier and cost-affordable access to it, it is very common nowadays for more and more organizations to utilize new technologies to support their businesses. Access to the internet and using the internet to access information remotely or collaborate with colleagues around the world from almost everywhere, the office, home, or when traveling, is now a commodity.

The use of new technologies can introduce new threats to organizations, which should be cautious and take appropriate measures to protect their businesses. According to the 2023 annual report of ISC2 on cybersecurity workforce shortages and skill gaps, 59% of cybersecurity workers said that skills gaps could be worse than total worker shortages. This number is even higher (67%) among workers whose organization actually has both skills gaps and total staffing shortages.

Organizations cannot afford to ignore the skills gap in the cybersecurity industry. Improperly trained cybersecurity professionals will not be able to assist organizations in protecting their valuable assets. For some organizations, that may turn out to be vital to their existence. As per IBM's 2023 "Cost of a Data Breach" report, the average cost of a data breach is $4.45 million, which has increased by 15% in the last three years. Organizations should ensure that they employ and retain properly trained cybersecurity professionals to avoid facing devastating cybersecurity incidents.

2). Is it a technical skills gap, a soft skills gap, or both?

It is a mix of both. Hard skills can be developed through professional education, certification training, seminars, or on-the-job training. The ISC2 study on cybersecurity workforce shortages and skills gaps shows a wider skills gap in new technologies, such as cloud computing security, artificial intelligence/ machine learning, and zero trust implementation. The ISACA-related report shows there is an increased need for identity and access management (49%), cloud computing (48%), data protection (44%), incident response (44%), and DevSecOps (36%).

Throughout my professional life, I have seen many professionals who are highly equipped with hard skills but lack the appropriate soft skills to work within a team or collaborate with others effectively and efficiently. Thus, having the appropriate hard skills is not the only thing that organizations should worry about.

The ISACA report shows that the top five missing soft skills are communication (58%), critical thinking (54%), problem-solving (49%), teamwork (45%), and attention to detail (36%). Soft skills can be developed through a collaborative approach that involves hands-on training, mentorship, and volunteerism.

Whatever the approach and whichever skills are missing, one fact is certain; any kind of skill needs time to be developed properly. The need is now.

3). Does the skills gap lead to greater cybersecurity risk?

Looking at the World Economic Forum's Global Cybersecurity Outlook report, published in January 2024, the impact the skills gap has on businesses is alarming. 36% of respondents list the skills gaps as the main challenge to achieving their cyber-resilience goals. Mid-sized businesses report that 61% lack dedicated cybersecurity experts, and only 9% claim their workers adhere to critical security best practices. These businesses evidently struggled to implement basic training measures and recruit the necessary staff.

Cybersecurity attacks have been listed within the Top 5 Risks of the Word Economic Forum's Global Risk Report for several years now. As per GCHQ, the UK's intelligence, security, and cyber agency, new technology, such as AI, is already being used to improve and increase the number of attacks targeting individuals and organizations. An increase in the severity of cyberattacks is expected within the next two years. Cloudstrike's Global Threat Report shows a 75% increase in cloud intrusions. All these facts show that the attack landscape is increasing and is expected to increase more in the upcoming years.

In addition, increased regulations, especially in the EU, such as GDPR, NIS 2, DORA, AI Act, and DSA, add even more burden to organizations to keep up with their regulatory requirements.

It is then a fact that organizations will face many challenges within the near future to protect their businesses. With the cybersecurity shortage and skill gap, organizations are struggling to sufficiently address cybersecurity threats leading to an increased cybersecurity risk.

Organizations should take immediate action to prioritize and address this cybersecurity risk, which is one of the many business risks they face that can have a severe impact on their sustainability. Techniques such as up-skilling and re-skilling current employees through professional education and certifications can prove vital to sufficiently addressing the risks to acceptable organizational levels.

Karla Reffold

Chief Product Officer

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

I am not as concerned about the skills gaps as I was 5 or 10 years ago. There are now a plethora of training companies and solutions that enable people to upskill in cybersecurity very easily. We are also starting awareness and training at a much younger age, giving elementary school children a route to learn some of the basics of cybersecurity. I think we have a pipeline of people who are interested in cybersecurity and an effective way of educating them. Many industry fields have a triangular career path. There are many entry-level jobs and few senior jobs, with openings decreasing as people become more senior. Cybersecurity is more of a rhombus right now. There are few entry-level and senior roles, but many for mid-seniority applicants. This means that cybersecurity hiring managers need to attract people with experience by creating compelling job opportunities. Or they need to be willing to retrain people from relevant disciplines. There is a lot of industry discussion about the need to create more entry-level jobs.

However, many of these discussions overlook some of the opportunities that exist. Many threat intelligence companies will hire junior analysts who have no experience. Managed Service Providers are another option where people can get hands-on technical experience, including cybersecurity experience. There are more jobs available outside of Security Analyst, Security Operations Center (SOC) Analyst, or Junior Pentester. The other solution that exists for companies who still struggle with hiring is automation. An increasing number of cybersecurity tools use automation to help limit the number of people required within a team. If you can automate processes and ensure that your current team is not overworked, you don't need to worry about the wider careers market.

2). Is it a technical skills gap, a soft skills gap, or both?

The cybersecurity industry has evolved to create roles that can be undertaken by someone with either soft skills or technical skills. For example, awareness-focused roles are well suited to someone with excellent soft skills. Penetration testers or malware analysts require more technical skills.

However, to truly excel, people need both skills, albeit not in equal measure. A CISO is unlikely to be successful (or even hired) if they do not have strong soft skills and the ability to translate technical issues into business issues. There are many client-focused roles, or roles where someone with deep technical knowledge needs to be able to communicate with the wider business. This is where there is the most demand and, often, the highest salaries are. There is a growing understanding of people who have excellent technical skills but weaker soft skills. As a society, we are more understanding of those who might be neurodivergent or who learn differently. This increasing acceptance that people learn and communicate differently is benefiting us all. This also helps the cybersecurity industry attract people and maximize the skill sets that people bring.

3). Does the skills gap lead to greater cybersecurity risk?

If you have a skills gap within your team, you are increasing your cybersecurity risk. A team with too many vacancies is going to burn out or be unable to keep up with the necessary tasks that keep the business secure. Also, consider the diversity within your team. There is strong evidence that a more diverse team makes better decisions and improves security. A diversity gap is as much of a risk as a skills gap. When hiring, businesses need to consider the time and cost difference between training and a lengthy hiring process. If finding someone with the right experience takes longer and costs a lot, you may be better off training someone yourself. With so many solutions to upskill employees in cybersecurity, this can be a good option that doesn't have to take time away from the current team. There are also plenty of cybersecurity professionals looking for remote jobs or strong benefits packages. Consider how competitive you are if you are struggling to hire. Automation and outsourcing are other options to mitigate any gaps. Threat intelligence and SOCs are great examples of something that can be outsourced. Attack surface management or vulnerability management are examples of things that have strong automated solutions available. Gaps in your team do make you less secure, but you have options to mitigate that risk.

Dimitris Georgiou

Chief Security Officer & Partner of Alphabit

LinkedIn

1). Should companies be worried about a skills gap in the cybersecurity industry?

The cybersecurity skills gap is not just about filling seats. Lacking security staff with experience and numbers has serious repercussions for organizations of all sizes. Cyberattacks are evolving at breakneck speed, and seasoned security engineers possess the battle-tested knowledge and intuition to recognize and thwart complex threats that might slip past less experienced personnel. And when experienced defenders lack in numbers, burnout looms. Stretched thin, critical staff risks exhaustion. Even though automated security tools are valuable in providing assistance, human expertise is irreplaceable. Tools cannot replace human judgment. Experienced engineers can analyze data, make critical decisions under pressure, and adapt to unforeseen situations, something automation struggles with. Furthermore, the ability to pass on knowledge and skills through mentorship to create the much-needed staff from within is an irreplaceable capacity. Seasoned security engineers can mentor and train junior team members, fostering a culture of cybersecurity awareness within the company, which creates a stronger overall defense.

2). Is it a technical skills gap, soft skills gap, or both?

The cybersecurity skills gap is both a technical skills gap and a soft skills gap. The technical skills gap refers to the lack of professionals with the specific technical knowledge and experience needed to handle cybersecurity threats. This includes expertise in areas like network security, incident response, digital forensics, penetration testing, and cloud security. The soft skills gap, on the other hand, refers to the lack of essential non-technical skills needed to excel in cybersecurity roles. These include critical thinking, communication, problem-solving, teamwork, oral and written expression, and the ability to work under pressure. Both are equally crucial since organizations need the technical knowledge to understand threats, implement security solutions, and troubleshoot problems. However, soft skills make a whole lot of difference as well; even the most technical expert can't function effectively without strong communication, teamwork, and the ability to analyze situations and make sound decisions while sometimes under immense pressure. Organizations need to address both aspects of the cybersecurity skills gap to build a truly robust cybersecurity posture.

3). Does the skills gap lead to greater cybersecurity risk?

The shortage of skilled cybersecurity personnel is a recipe for trouble, with cybersecurity risk increasing proportionately to the size of the gap. Without enough qualified personnel, companies struggle to keep up with critical tasks like patching vulnerabilities and monitoring for suspicious activity. This leaves them exposed to known exploits that malicious actors can easily exploit. Simply put, each missing cybersecurity professional is a hole in the castle's wall. Attackers can infiltrate, remaining undetected for longer periods, potentially stealing sensitive data or disrupting operations. Even when a breach occurs, the lack of experienced professionals can lead to a slow and ineffective response. Think of a data center breach with an understaffed security team. The attackers have more time and freedom to roam and cause damage while the defenders scramble to understand and contain the issue. Further, overworked and understaffed security teams are more prone to burnout and critical errors. Imagine a single security analyst monitoring a massive server farm at night, constantly fatigued and overwhelmed by incoming events. Exhaustion can cloud judgment, leading to missed security alerts or misconfigured responses. This creates an additional layer of vulnerability exactly where the critical decisions are made; at the human level.

Conclusion

The cybersecurity skills gap is a significant issue that deserves the industry's attention. It increases the risk of security incidents, results in higher staff burnout, and sends business costs sky-high. Initiatives like training and mentorship programs, government and industry collaboration plans, and diversity and inclusion strategies will be fundamental to closing the skills gap over the coming years.

While the experts believe the industry will never eliminate the skills gap, it's clear that most of them are cautiously optimistic about the future.