Bridging the Skills Gap in the Cybersecurity Industry
Cyber criminals are becoming advanced than ever before, forcing companies to increase their response through a skills cyber force. During these uncertain times cybersecurity is of increasing value to businesses, especially as remote working is becoming a norm in many societies. Whilst the importance of cybersecurity is rising, so are the number of job vacancies within the sector. The demand for cybersecurity professionals outweigh the supply of individuals to fill in those roles, due to the large gap in skills.

Every 39 seconds a cyber attack occurs, costing firms an average of $13 million.
Whilst there has been a drop, IBM predict that the skills gap in the industry will reach **18 million** by 2022, showing no sign of shrinking. There are many reasons for this wide gap, one of them being the lack of training and investment in training of individuals.

In order for the talent gap to be filled, employment in the field needs to grow **89%** worldwide, forcing companies to introduce different initiatives in the workforce.

According to the 2020 Cybersecurity Workforce Study, the skills gap in cybersecurity has **shrunk from 4.07 million to 3.12 million**.
An organisation is only as good as its people, and 3 out of 4 cybersecurity professionals believe that there is not enough investment in training individuals. 76% of cybersecurity professionals were IT professionals before, so lack the skills and knowledge needed to use cybersecurity technology to its full potential. Cybersecurity staff are overworked, lack skills and companies are relying on those marginally skilled individuals for advanced requirements, widening the skills gap.
70% of cybersecurity professionals claim that their organisation is impacted by the skills shortage. Many organisations find it difficult to upskill employees, or find the time and resources to train new employees when they are dealing with an increase in cyber attacks. The underinvestment in training and education, as well as the escalation of cyber threats increases the dire need for skilled individuals. 58% of cybersecurity professionals believe that their organisation should be doing more to train individuals on appropriate protocol.

The skills gap exists because an individual’s technical capabilities do not evolve with technological advancements, making companies require both knowledge and experience that is limited. Many blame the skills gap on the lack of skilled applicants, instead of focusing on the responsibilities of organisations to train employees. The cybersecurity industry faces a lack of both training and career development opportunities, making it unattractive for potential employees. 68% of cybersecurity professionals say they lack growth activities, certifications and mentors, blurring their career path. Such professionals feel constrained by the lack of future development, indicating that organisations lack strategic planning when it comes to cybersecurity.
PWC’s 2018 CEO survey found that both the availability of skills and cyber threats is one of the top 5 threats to business growth prospects. As aforementioned, cyber attacks occur every minute, and this is especially enhanced in light of the pandemic. 76% of survey respondents find that the skills shortage has created additional risks for their organisation, one of them being cyber crime vulnerabilities. 90% of cybersecurity professionals believe that organisations are vulnerable to significant cyber attacks. Many industry professionals believe that the rise in cyber attacks is overwhelming individuals, especially those who lack skills.

A study showed that the skills shortage the industry is faced with is a key factor in a number of data breaches. Non-technical Individuals who lack the appropriate training and skillset are unable and unaware of the ways to deal with data breaches and cyber attacks, making their organisation extremely vulnerable. Without the proper protocol, individuals are unable to protect their organisation, widening vulnerabilities as well as the skills gap in the industry.
The demand for cybersecurity skills outweighs the supply, forcing companies to invest time and resources in training new and current employees. Organisations can close the skills gap by empowering cybersecurity professionals to expand their skillsets and continue to grow beyond current roles with the help of on the job training, mentoring programs and financial incentives. As cybersecurity is constantly evolving, companies have to change the way skills are educated, and the way talent is assessed. Organisations need to build a talent pipeline for cybersecurity with the help of apprenticeships and internships. The needs of the industry are constantly changing, as such employees need to be upskilled. Through investing in training, individuals are kept up to date on latest threats and software. This increases the chances of strong security practices, as well as the skills of individuals, providing them with the tools to see beyond alerts, making fundamental changes that are essential for proactive defences. In doing so, organisations are providing a path for entry level staff to increase their knowledge and experience, thus increasing their loyalty.
Furthermore, to bridge the gap organisations must be better at spotting and nurturing the right talent. Thus far, organisations have been looking for cybersecurity specific skills, overlooking other transferrable skills that could be of value. The focus on industry specific experience is only widening the gap. In this age of digital transformation, the shortage of skills is no longer an inconvenience, but a threat. As such, organisations must now look at individuals from non-traditional backgrounds who bring a new perspective to the industry, as IBM have done. Looking at upskilling employees from different sectors of the business, such as IT, adds value to both the organisation and the individual. In prioritising a variety of skills and knowledge, organisations are hiring individuals with qualities that can’t be taught in a classroom.
Contact Us Today:

WEBSITE
www.advisorykonnect.com

EMAIL
info@advisorykonnect.com

CONTACT NUMBER
+44 (0) 203 371 7394