Picture credit: AdobeStock

THE AI EFFECT

Richard Woolfrey *outlines ways to bridge the cyber skills gap in the age of AI*

The UK is facing an unprecedented escalation in cyber threats. Research from the National Cyber Security Centre (NCSC) shows that "four nationally significant" cyber attacks take place each week – an indication of how threat activity is embedded into daily life. Organisations across every sector, from retail to manufacturing, education and even critical national infrastructure, are feeling the impact with these incidents having major consequences such as disrupting operations, jeopardising trust and financial stability as well as threatening the UK's broader national resilience.

In the past twelve months alone, 86 percent of organisations have experienced one or more security breaches, demonstrating how the speed, sophistication and severity of attacks have intensified. Part of this rise is due to a new cyber security 'norm' in which threat actors operate with advanced tools, automated techniques and innovative technologies. Among these, AI stands out as the most transformative.

AI is reshaping the cyber landscape on two fronts. On one hand, 49 percent of organisations are concerned it will increase cyber attacks, since it's already being used to aid highly targeted cyber criminal activity. On the other hand, AI presents significant opportunities to strengthen defences and relieve pressure on over stretched security teams struggling against a growing global skills shortage. With threats rising and attacks evolving, organisations must ensure they have the right tools and, critically, the right workforce to defend against them.

Globally, there is a shortage of 4.7-million cyber security professionals

Cyber security teams are stretched. Globally, there is a shortage of 4.7-million cyber security professionals, but this skills gap has become more than solely a supply and demand issue that can be solved by traditional recruitment alone. As the threat landscape evolves, so must the way organisations attract, train and retain talent.

Today's cyber skills shortage impacts organisations in two critical ways. First, there are simply not enough trained specialists to fill essential technical roles, such as security analysts, cloud security engineers and incident responders. These jobs require deep and often niche, expertise. Yet, the talent pipeline is not expanding at the pace required to meet demand.

Second, even within organisations with established security teams, there is a widespread lack of cyber security awareness among non-technical employees. The result is an environment where security teams bear significant pressure while everyday staff can create vulnerabilities, falling for scams for example.

Together, these challenges pose very real consequences. 67 percent of organisations report the skills shortage creates additional risks for their businesses and 56 percent of IT decision makers state that a lack of cyber security awareness in employees is the top cause of breaches. The combination of too few expert practitioners and too little everyday security literacy is creating vulnerabilities threat actors are increasingly able to exploit.

Making this issue even more complex is the pace at which digital transformation is accelerating. As organisations adopt cloud services, edge computing, IoT and AI-driven applications, the number of systems requiring protection grows. This creates a moving target and security teams need to constantly adapt and upskill to defend new and unfamiliar technologies and threats.

Despite thousands of cyber security roles going unfilled each year, many potential candidates hesitate to apply for roles. The reason is simple: they feel they lack the required qualifications or experience. This perception is often reinforced by employers, with 52 percent still considering whether a candidate has a four-year degree when hiring.

This approach of favouring traditional pathways restricts the talent pool, but also prevents organisations from embracing applicants from a wider range of backgrounds and educational pathways. This is despite many having strong potential or relevant capabilities.

To close the growing skills gap, the industry must start seriously considering candidates from programmes and schemes, such as apprenticeships, vocational programmes and skills-based assessments, which offer alternative routes into the profession.

The examples of veterans illustrate this well. Figures have found they and their spouses remain considerably harder to recruit at 43 percent and 41 percent respectively, yet, they often already have the skills cyber security companies desperately seek. Alongside this, there are parallels between what the military and cyber security professionals do – use intelligence and defences to defeat attackers. Positively, the industry is beginning to adapt. We're seeing organisations starting to tap into talent from less traditional pathways, like apprenticeships – 65 percent of employers claim to be prioritising professional certifications over academic qualifications. Certifications are an effective way to validate practical, current skills and demonstrate a candidate's readiness for real-world responsibilities.

However, this should be considered only as the starting point. Other credentials and training options must also be considered, especially when organisations are willing to invest in on-the-job development. By broadening the criteria for entry into cyber security roles, the industry can ensure it is accessing the best and brightest talent capable of keeping us secure.

AI CAN ENHANCE SECURITY AND HELP MITIGATE RISK, BUT PEOPLE MAKE THE DECISIVE DIFFERENCE

In addition to improving entry routes, organisations need to build clearer internal pathways for career progression. Many great candidates enter cyber security roles to find limited opportunities or unclear structures around advancement. Implementing validates competency frameworks and clearly communicating career trajectories, businesses can better retain talent.

For job seekers or those looking for a career change, this creates more accessible routes into the industry. Pursuing certifications, practical training and upskilling allows individuals to position themselves competitively in the market. For organisations, embracing these pathways will create the diverse, skilled workforce the sector urgently needs to stay ahead of the constantly changing threat landscape.

AI literacy isn't only for security professionals. With AI now deeply integrated into daily workflows and consumer technologies, without the knowledge to use AI responsibly, employees risk exposing organisations to accidental data exposure, misinformation and AI-enabled scam campaigns.

Concerns surrounding AI misuse are rising and there is growing unease around how threat actors are using this innovative technology to develop more sophisticated, automated and targeted attacks. We are already seeing cyber criminals using AI tools to create deepfakes, automated phishing campaigns and adaptive malware – Anthropic recently identified a new era of espionage, with hackers trying to infiltrate AI platforms to attack Western businesses.

This also highlights the need for organisations to build robust AI governance structures, including setting clear AI use policies and regular training around AI risk. AI literacy should include understanding of the limitations of AI outputs so workforces can make informed choices around when and how to use the technology.

In response, the adoption of AI-powered cyber security tools for protection is accelerating. Whether

it's threat detection and prevention, security automation or behaviour analytics, 97 percent of organisations are using or planning to use AI-enhanced cyber security solutions. Moreover, three quarters of organisations that experienced nine or more cyber attacks in 2024 are already using AI tools, showing that repeated incidents push faster adoption.

67% OF ORGANISATIONS SAY THE SKILLS SHORTAGE CREATES EXTRA RISKS FOR THEIR BUSINESSES

Yet, technology alone isn't enough. As many as 48 percent of IT decision makers say insufficient AI expertise among employees is the biggest challenge to integrating AI into cyber security programmes effectively. Without AI literate workforces, organisations risk misusing tools, misinterpreting results or failing to detect AI-driven threats.

To counter this, organisations must invest in upskilling workforces through targeted training in both AI and cyber security. A workforce equipped with both technical and contextual understanding of AI's capabilities will be better prepared to maintain security, use AI responsibly and help their organisations stay resilient.

AI is reshaping cyber security faster than any previous technology. This evolution makes the current skills gap more than a workplace challenge: it is a strategic threat.

We know organisations require skilled professionals with strong AI expertise and workforces with better AI literacy to equip them to operate safely in the new digital world. To build this resilience though, they must invest in upskilling employees; encourage continuous learning and certification pathways; adopt hiring practices that value skills, potential and practical capabilities as much as formal education; and empower every employee to play an active role in protecting against threat actors.

For workers, AI represents an opportunity as much as a challenge. Those who develop AI and cyber security competencies can futureproof their careers and stand out in a competitive, high-demand job market.

Alongside this, to be truly future-ready, businesses must understand that cyber security needs to be embedded into organisational culture, rather than confined to specific teams. Cyber security should be a shared responsibility across departments, and leadership teams need to model the behaviours they expect their teams to follow. By making security part of an organisation's DNA, employees will be empowered to do their bit to keep the business secure.

The cyber security and AI revolutions are happening simultaneously, presenting both significant risks and unique opportunities. Recognising the skills gap is only the first step in identifying how to close the door on threat actors infiltrating organisations. What truly matters is how organisations respond – investing in people, developing new pathways into cyber security and building a workforce that is both diverse and AI-literate.

While AI technologies can enhance security and help mitigate risk, it is people who will make the decisive difference. Organisations that build strong, adaptive and skilled cyber teams will be best positioned to protect operations, safeguard customers and secure a resilient digital future. Building an AI-literate workforce is simply not an option; it is the only sustainable path to long-term security ●

Richard Woolfrey is the Regional Director for Fortinet in UK and Ireland.

Military veterans often already have the skills cyber security companies desperately seek

Picture credit: Crown Copyright