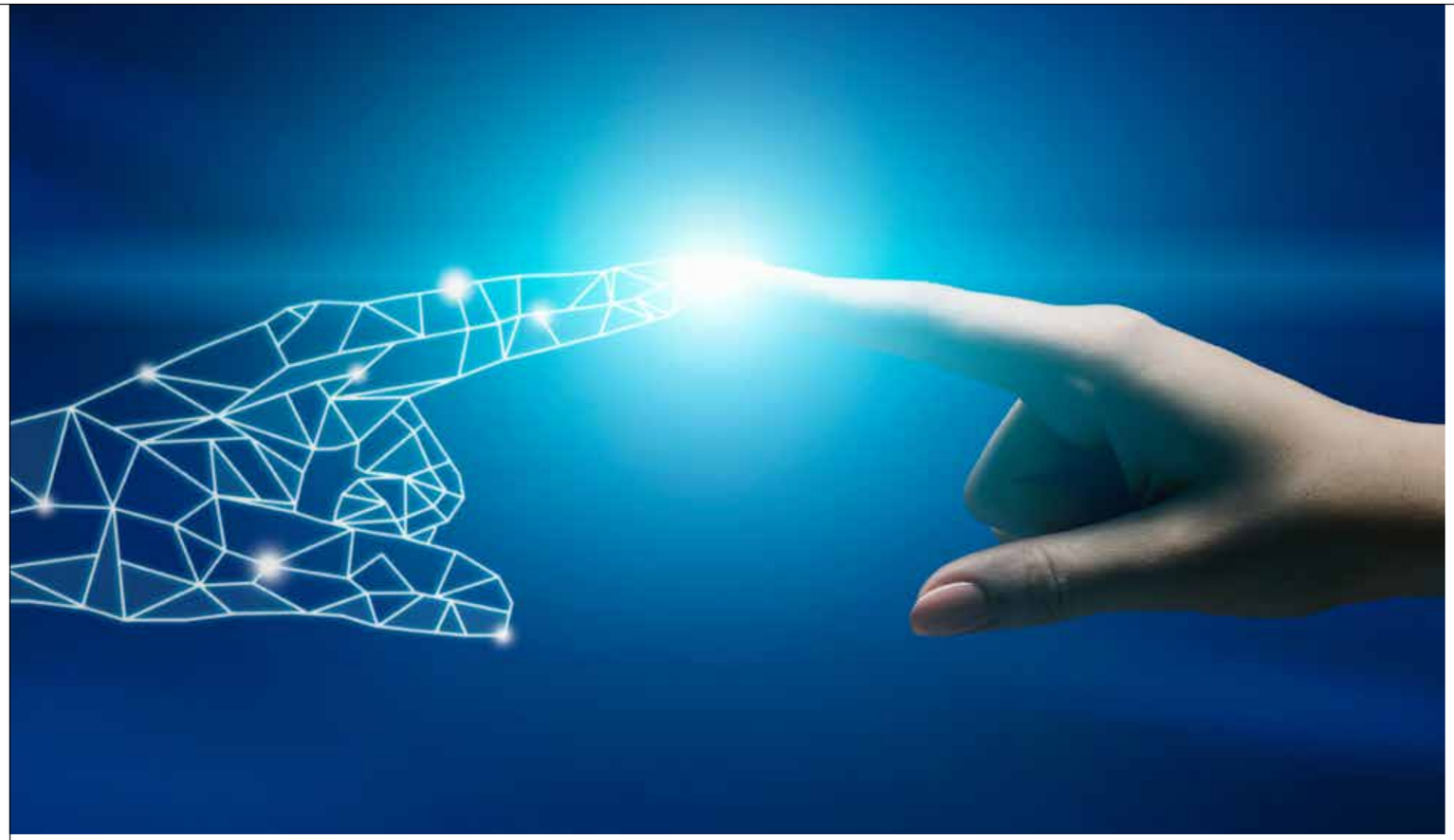

Picture credit: Adobe Stock

HELPING HANDS?

Jamal Elmellas *explores the role of technology in creating and solving the cyber skills shortage*

The cyber security skills gap rocketed by 73 percent in the UK according to the ISC(2) 2022 Cyber security Workforce Study and it's showing no signs of abating, with the Department for Digital Media and Sport (DCMS) estimating an annual shortfall of 14,100 new entrants needed into the field. But, at the other extreme, we're also seeing something of a mass exodus due to the 'great resignation' that followed the pandemic, with 4,600 people leaving annually, as well as widespread stress and disillusionment. According to The State of the Security Team 2022 report, work-related stress is increasing in nearly 70 percent of companies, with 30 percent reporting a significant increase.

A key cause of this stress is the technology that cyber security professionals rely upon to do their jobs. The same survey found that aside from more staff and support, the respondents thought better integrated security tools would alleviate their stress. This is understandable given that it goes on to reveal that 85 percent of businesses had deployed overlapping security solutions, unintentionally, meaning security teams were having to deploy and maintain systems that duplicated results, yielding no real gains in terms of defence or response times.

The exodus of cyber security staff means a loss of experience and knowledge on how legacy systems work

Increasingly, cyber security professionals are having to monitor security stacks comprised of multiple proprietary point solutions of anything between 20-70 tools. In order to do so, they need to learn how those work, often resulting in non-transferable skills, and the solutions themselves often generate high false positive rates, leading to alert fatigue. Altogether this is resulting in high burnout rates, with The Global Incident Response Threat Report revealing that over half feel extremely stressed with 65 percent considering quitting.

There's also not enough training being offered to help employees upskill and progress, further frustrating their ambitions. The majority of unfilled job roles are for those at the managerial level with between three or more years' experience, according to the DCMS Cyber Security Skills in the UK Labour Market 2022 report, which means this failure to invest will have long term consequences. The Pulse: Emerging Technology 2021 report by ISACA found that 48 percent think there is not enough investment in training to move with the changing technology landscape, while the The Life and Times of Cyber security Professionals 2021 survey found nearly a quarter were not receiving the 40-plus hours training per year needed to maintain and advance their skillsets. This paints a bleak picture for the future.

From a technology perspective, the exodus means a loss of experience and less of those around who know how these systems work. This is particularly true for legacy systems, for example, mainframes are still used for mission critical processes in sectors such as banking, telecoms and retail, with IBM revealing 67 out of out of the Fortune 100 rely on them. The likelihood is that these systems will continue in operation for at least another decade while these businesses digitally transform yet those with the skills to maintain them are in increasingly short supply, with few new entrants keen to learn a dying language.

While it's becoming increasingly difficult to manage existing infrastructures, it will also be very difficult to move forwards and to adopt new technology, particularly given current economic conditions. According to a NISC survey, 69 percent of respondents think current budget constraints are limiting the use of new strategies, technologies and implementation practices and 49 percent don't have the budget to meet current cyber security needs. This effectively puts businesses in a state of limbo, but could also make them more vulnerable.

Attackers, funded by organised crime and nation states, will not be disadvantaged in the same way, meaning they are well positioned to exploit any slip in security. Indeed, a survey by the World Economic Forum found 60 percent think the skills shortage will compromise the security team's ability to respond to a security incident.

However, while technology may have proven a draw on human resource up to this point, the hope going forward is that it will help to alleviate workloads. Automation in the form of machine learning and AI is now beginning to make an impact from continuous monitoring solutions and threat detection for incident response to automated security testing and compliance.

In theory, these solutions should free up time, enabling professionals to do more high-level demanding tasks. They can automate many of the important but mundane processes such as the monitoring and analysis of network logs, if configured correctly, and doing so boost staff morale. However, confidence remains low, with only 17 percent believing that AI, machine learning and automation will help to address the skills gap, according to an ISC(2) 2022 Cyber security Workforce Study.

That said, the survey took place before the release of ChatGPT and other forms of Generative AI. This is proving to be a real disruptor as a technology, although the jury is still out on who stands to gain. While it will undoubtedly be used to make security processes such as reporting more efficient, it could also prove a boon to attackers with a report in the *New Scientist* claiming it could cut costs by up to 96 percent for organised criminal gangs by enabling them to craft convincing phishing campaigns.

BUSINESSES NEED TO OFFER THE TRAINING NEEDED TO SPECIALISE IN CYBER SECURITY AREAS

Also on the horizon is the prospect of Quantum Computing, which promises to take AI to new levels. It will see lightning speed processing (it's already been used to solve a problem in 200 seconds that would have taken 10,000 years on a normal computer) and so will be able to fast track the learning of AI systems, which currently take months to train. Of course, Quantum Computing does raise other issues, such as the need for an alternative to current methods of encryption, all of which will effectively become compromisable and therefore redundant, with NIST already looking at four contenders. So expect a seismic shift in the use of technology in cyber security within the next ten years.

Back to the here and now, and the current focus given the bloated cyber stack and emphasis on conserving spend due to economic pressures is consolidation. According to a Gartner report, *The 2023 Leadership Vision for Security and Risk Management Leaders*, 75 percent of CISOs were pursuing a vendor consolidation strategy last year compared with just 29 percent in 2020. That's good news for cyber security personnel because it means companies will seek to limit the number of vendors they use, as they seek to combine solutions and prioritise third party integration and open standards. This should help to whittle down the security stack, meaning less systems to monitor, and see professionals benefit by being able to utilise their skills when they switch employers.

Of course, these technological changes will all create a constant moving feast of skills in cyber security. Today we're finding there are not enough people in emerging disciplines, such as cloud, AIOps (artificial intelligence for IT operations) and DevSecOps (development and security operations). Fortinet's *2022 Cyber security Skills Gap* report found half of organisations globally are looking for cloud security specialists, 42 percent SOC Analysts and Security Administrators and 40 percent Security

Architects, while the ISACA *State of Cyber security 2022* report found the top-five security skills in demand today are cloud computing, data protection, Identity Access Management, Incident Response and DevSecOps.

To help fill these gaps, businesses must refine their retention and recruitment strategies. They should stop looking for 'off-the-shelf' candidates that come ready trained and experienced or posting 'unicorn' job ads and must instead be willing to offer the training needed to specialise in these areas and to provide a career path offering progression within the company. Look internally, too, and earmark candidates for training and promotion and even consider cross-recruitment from other departments.

THERE ARE SIMPLY NOT ENOUGH PEOPLE IN EMERGING CYBER SECURITY DISCIPLINES

Thus far it's clear that technology has been focused on improving the security posture of the organisation but often at the expense of the workforce. Recruitment processes have been too narrowly focused with employers favouring experience over aptitude, meaning potential candidates are overlooked and excluded from the process. Going forward, the hope is that technology will help to correct these issues and become the enabler that allows people's careers to thrive and acts as an incentive, encouraging them to remain in the sector.

It's imperative that we do, because it's not just the cyber security gap that is growing larger. Data is increasing exponentially and with it the ways in which it is created and shared, and with that proliferation comes a more distributed architecture and a larger attack surface. Unless we learn to use the tools at our disposal more efficiently to make up for the shortfall of skilled cyber security professionals and to equip those we have, we cannot hope to cope with this scale in demand.

The State of the Security Team 2022 report wisely surmises that more attention needs to be paid to frontline security staff and that means focusing on three things: consolidation, training and staff retention. All three strategies not only put the needs of the security team first and foremost, but also align with the need to conserve spend and focus on investment that futureproofs the business at a time when budgets are tight.

We need to stop thinking about how we can create a funnel of more people and start thinking about how we can support and technologically arm those we have, make their working lives more rewarding to encourage them to stay and the roles more enticing to those coming into the market through clear career paths and progression. To achieve that, we need to harness our technology better and only then can we hope to solve the skills crisis ●

Jamal Elmellas is Chief Operating Officer at Focus on Security, the cyber security recruitment agency, where he is responsible for delivering an effective and efficient selection and recruitment service. He has almost 20 years' experience in the field and is an ex CLAS consultant, Cisco and Checkpoint certified practitioner.

The hope going forward is that AI and machine learning will help to alleviate workloads

Picture credit: Adobe Stock