UK agencies respond to challenge of recruiting and retaining cyber-skilled staff

Cyber security is a top-tier threat for the United Kingdom, but national intelligence and law enforcement agencies face a 'cyber skills gap' when it comes to recruiting and retaining specialist staff. *Matthew Redhead* assesses the UK agencies' efforts to build a new 'Generation Cyber'

Key Points

- Government agencies in the UK and abroad face the dual challenges of recruiting enough people with technical and practical cyber skills, and of retaining those staff as they advance through their careers.
- National skills development strategies are likely to gradually reduce the recruitment challenge, but the retention issue is likely to prove enduring for agencies given the disparity between public- and private-sector wages for cyber roles.
- Agencies will therefore either be forced to accept considerable turnover among staff with cyber skills, or adopt novel approaches to meeting these skills gaps, such as greater integration with the private-sector cyber-security 'ecosystem'.

The demands of cyber security are changing political, military, and security structures at a rapid pace. On 31 July 2019, the British Army announced that it was recreating its 6th Division, explicitly to tackle cyber issues from hostile states. This increasing concern around the exploitation of the 'cyber domain' (see box) by overseas powers – but also by terrorists, serious organised criminals, and radical 'hacktivists' – has generated a high demand across the UK public and private sectors for individuals with cyber-security skills to protect the country's cyber estate and, increasingly, to take on its attackers.

However, the UK currently faces an acute cyber-skills shortage. As one former UK government technology specialist told *Jane's* on 19 July, "Cyber skills demand now massively outstrips supply, because everyone is waking up to the threat at the same time." This 'supply line' problem also affects the specialist cyber recruitment of the UK intelligence and law enforcement agencies, employment in which is further burdened with the lower comparative pay than in the private cyber sector, and the length of the vetting process. These negatives are often initially offset for new recruits by the 'mission kick' of working on national security challenges, but the retention of specialist cyber staff becomes challenging as domestic financial demands increase – such as buying a home or having children – and pay differentials with the private sector widen.

In response to the national cyber skills challenge, the UK government announced in 2018 that it was drafting a National Cyber Security Skills Strategy, due for issue in late 2019. The

Skills Strategy will seek to build on previous efforts, often fostered by the intelligence agencies, to work with businesses, schools, and universities to increase the supply of young cyber talent. Government Communications Headquarters (GCHQ) and other agencies have also worked through such dedicated educational and apprenticeship schemes to identify suitable candidates for their own staff, mirroring similar efforts by defence and security agencies in countries such as Estonia, France, and Israel.

Social networks continue to diversify and increase in complexity. Government agencies are facing challenges in identifying individuals with the skills needed for a range of practical and technical cyber-security roles. (dem10/Getty Images)

1744790

Jane's assesses that these efforts are likely to improve – gradually – the overall stock of cyber-security skills in the agencies. However, staff retention is likely to remain a more intractable problem, as pay differentials and cultural differences between the public and private sector are unlikely to change in the near term. In the longer term, this could prompt a more radical approach to cyber skills retention, allowing a more fluid 'ecosystem' of specialist deployments to develop between the public and private sectors.

UK cyber-skills gaps

According to a 2018 study by technology consultancy CapGemini, the UK had the third highest share of "global cyber talent" (13%), well behind India and the US, but ahead of France and Germany. However, separate research by Ipsos MORI in 2018, sponsored by the Department for Digital, Culture, Media and Sport (DCMS), found that there was still a pronounced domestic gap within the UK, with 54% of businesses and charities and 18% of public-sector organisations lacking "basic cyber-security skills".

What this gap in reality amounts to is somewhat ambiguous, because the definition of basic cyber-security skills in the Skills Strategy document is very broad. It includes expertise in strategic management, planning and organisation, investigative and 'soft' skills, and data protection, in addition to the technical areas traditionally understood to constitute cyber-security skills. These range from the conceptual understanding of operating systems, programming languages, and networks, through to experience in system architecture design, encryption, incident response, and forensic investigation.

Speaking to *Jane's* on 25 July, Cameron 'Buck' Rogers, Professor of Cyber Security at Gloucester University and former Chief Information Security Officer (CISO) of the Bank of England, commented, "Not all cyber skills are the same. Some cyber security roles demand exotic technical skills, but the vast majority do not; in many cases it's more important to have an understanding of risk management and the pitfalls of human psychology than advanced computer science." In essence, there are therefore two broad types of gap: the technical, and what might be described as the 'practical'.

In an interview with *Jane's* on 24 July, Ed Parsons, Managing Director at cyber consultancy F-Secure Consulting, outlined the technical dimensions of the skills gap, saying, "The UK has had an historic issue with getting enough young people into STEM [science, technology, engineering, and mathematics] subjects." He noted that this situation was slowly beginning to improve. Indeed, according to the UK's 2019 A-Level results, published on 15 August, the upward trend in young people taking science-based subjects over arts and humanities has continued, although with girls some way behind boys on subjects such as computing.

However, according to Parsons, the pool of STEM-educated talent suffers heavy attrition before it ends up in cyber security. "There are alternatives to cyber at every stage," he noted. "Artificial Intelligence (AI), robotics – even computer game design – we have to compete with these other industries for young people's attention."

[Continued in full version…]

(806 of 3520 words)