Reskilling the cyber gap in the UK

Cyber security trainer at QA Limited, James Aguilan shares his expert opinion on the key issues around reskilling the cyber gap in the UK today

McAfee, security firm, states that UK education systems are providing minimal insight into careers in cyber security. Government bodies have addressed the skills gap with plans to triple the amount of computer science teachers in schools and introducing a National Centre for Computing. CWJobs found that 65% of employers thought the government had not invested enough in training the next generation of tech employees, which is causing a gap in the field of cyber security. Notably, with recent high profile cyber-attacks including Uber and NHS data breach, the importance of robust cyber security is clear, or at least it should be. Here, I discuss the concern with cyber security gaps.

Skill shortage in secure coding, cyber security and cloud migration are widespread

The main concern for the shortage in cyber security is the inadequacy in preparing for the demands of technology, specifically, within secure coding and cloud migration. 31% of cyber security professionals state that organisations have a shortage of application security skills. When you think about the whole digital transformation trend going on across all industries, it's easy to conclude that this mismatch can only result in a lot of insecure code being developed and deployed.

Additionally, 29% of cyber security professional state organisation has a shortage of Cloud security skills. ESG research indicated that 42% of organisations currently use IaaS and/or PaaS services today and these percentages are poised to increase in the future. Beyond this, survey respondents point to a skills shortage in areas like penetration testing, risk/compliance administration and security engineering. The overall picture is bleak – many organisations may not have the right skills and resources to adequately secure new business and IT initiatives and may also lack ample skills to detect and respond to incidents in a timely fashion.

Lack of readiness for a cyber security attack

With numerous high-profile security breaches in recent years, UK businesses are facing greater pressure to ensure their security measures are up-to-date and in place. However, despite the increase in both attacks and warnings, many companies remain complacent as some believe they can't be hacked. As a result, they lack the right approach or plan to protect themselves against attacks.

With organisations confidence so low, it is unsurprising only 50% of small business enterprises (SME) are prepared for a cyber-attack. On the other hand, the other half of organisations are said to look for cyber security skills when recruiting new tech talent. Experis research found that 65% of employers thought the government had not invested enough in training the next generation.

Beyond the recent budget, however, the government has taken steps to address the problem of a skills shortage. For example, the UK Government launched the National Cyber Security Strategy in 2016, part of which incorporates a plan to make sure there is a constant supply of home-grown cyber security talent. However, 80% of technology organisations stated that they are currently struggling to fill cyber security roles, with 30% believing this is due to an industry skills gap.

Educating the cyber skills gap

In 2017, GCSE/GCE/Degree grades have marginally improved. However, there are still systemic issues when it comes to cyber security. So, how can businesses address the skills gap? Organisations can deploy an innovative recruitment process in a bid to resource the skills that they can't currently find. An example and a good place to start is implementing gamification.

The National Cyber Security Centre's (NCSC) codebreaking exercise is a playing field for all applicants – in that the recruitment process can be used to find prospective candidates from all backgrounds. Not only did it enable NCSC to see how well potential candidates would fare on the job, it gave them access to a larger pool of raw talent. In turn, this results in a greater

diversity of skills – an essential asset for any business looking to contend with a threat landscape that evolves by the minute.

Introduction to apprenticeships and The CyberFirst Programme

As an alternative to the traditional education system, another route to bridge the security gap is for businesses to offer apprenticeship programmes for young people looking to get into the industry. A cyber security apprenticeship programme involves the hiring of raw talent, after having completed their GCSEs or GCE. Apprentices can work, develop new skills on the job while learning and earning at the same time. This way, apprentices can study for the certifications they require, with businesses also getting the exact cyber security skills they need to protect their organisation from threats.

What's more, apprentices don't have to attend a university or college to do apprenticeships. Taking on apprentices is the perfect way for businesses to nurture a robust cyber security team that is fit for purpose and has the technical and practical know-how to fend off cyber threats.

Introducing cyber skills and awareness early - is often key to encouraging the next generation to consider cyber roles later. The CyberFirst Programme targets children from GCSE age onwards – CyberFirst is a collaboration between NCSC, QA and The Smallpeice Trust. It is a pivotal part of the UK Government's National Cyber Security Programme and aims to embed cyber skills to give talented young people the support, experience and exposure they need to become the cyber professionals of the future.

To prevent a worst-case scenario – technological change accompanied by talent shortages, mass unemployment and growing inequality – reskilling and upskilling will be critical. Every industry is being impacted by the rise in technology and an increased reliance on the Internet of Things (IoT). Thus, businesses are being forced to rethink the way they work and turn to new technologies to remain successful. The upsurge will see countless new roles created as employers seek digitally-savvy workers to help them master these technologies.

However, to thrive the modern employee will need to learn new skills and have some form of cyber awareness. Apart from a reform in basic education, it is simply not possible to weather the current technological revolution by waiting for the next generation's workforce to become better prepared. In its place, it is critical that businesses take an active role in supporting their current workforces through reskilling and upskilling. This approach of cross-collaboration between business sectors, the government and the education system are mandatory if millennials and future generations are to become the sharp, aware and talented cyber defenders our societies need.

James Aguilan
QA cyber security trainer
QA Limited
Tel: +44 (0)330 029 7735
Cyber.qa.com