FUELLING THE TALENT PIPELINE IN LONDON REQUIRES SERIOUS INVESTMENT IN CYBER SKILLS

By Dr Vahid Heydari Fami Tafreshi, senior lecturer in Cybersecurity and Networks, Computing Courses Provision Manager at Staffordshire University London

The cyber industry has grown massively in size over the last few years, and with cybercrime expected to cost our economy $10.5 trillion globally by 2025 the growth of the sector is not going to stop soon. This presents the UK and London with a massive opportunity to provide people with good highly paid jobs, but only if we can engage, attract and retain the best talent.

As the tech epicentre of the UK, London is home to a plethora of cyber start-ups, scale-ups and unicorns. Of the 1,221 cyber firms in the UK, London is the favoured destination for cyber companies to be headquartered in the UK, with 35% residing in the capital. To ensure this continues we must fuel the talent pipeline for the cyber sector, and make sure we have enough people with the skills required to fuel the industry.

Cybercrime comes in many forms, from fake public networks and phishing to malware and identity theft. But these threats cause more than just inconvenience. Cybercrime causes financial and personal harm to victims and the risk of exposure is far greater as people increasingly work, socialise and live on the internet.

Cyber-attacks have risen in frequency and severity. Cybercriminals have become increasingly more sophisticated as technology and innovation has developed. They have also taken advantage of people spending more time working at the home than in the office.

With the lack of smart systems at home, the potential of cyber threats has been exacerbated by the rise of hybrid and remote working during the pandemic. 70% of businesses have had increased exposure to cyber threats since the pandemic started making them more vulnerable to attacks. This is due to a number of factors, particularly unsecured and exposed cloud services and network servers.

This has led to the Government classifying cybercrime to be a Tier 1 threat when it comes to our national security, with new figures reporting losses of £91.2m to London's citizens and businesses in H2 of last year. To fight cybercrime, we need businesses to invent innovative solutions to tackle it, and to achieve this we need to supply growing firms with the talent they need to build products to protect the market.

We're going to have to work hard to meet the demand because we have a growing digital skills gap in the UK. A report from the Open University highlights this, with organisations in the UK spending more than four billion pounds a year as they are unable to find employees with the right skills – with more than 68% of employers struggling with this problem.

Recent data from Tech Nation has also spotlighted the immense number of vacancies for jobs within the digital sector. This is particularly the case for the cyber sector. Whilst advertised tech roles in the UK grew 36% as of June 2020, the number of searches for 'cyber security jobs in the UK decreased by more than 1,000 searches in a single month in 2020. We need to not only inspire people to pursue a job in the sector but make sure they have the skills to match.

The growing number of unfilled vacancies can be traced back to one main issue. This is a lack of digital skills making the pool of talent to fill tech vacancies increasingly small. In fact, 3 in 20 UK employers face a digital skills crisis, and with 82% of all jobs in the UK listing digital skills as a requirement, it is clear something is misaligned.

Many jobs that will exist in 2030 have not even been invented yet - including in the cyber sector. This means it is important we teach young people tangible transferable skills in tech that can be applied to many different industries. Universities can play a key role in making sure people have the skills required for the future of work.

Here at Staffordshire University London, we make digital skills training the ultimate priority. As one of the first universities in the UK to provide an undergraduate Cyber Security degree offering training in areas from cybersecurity to forensic computing, we believe digital skills will future-proof people's career paths.

By partnering with the likes of Cisco, Juniper, Microsoft, Amazon, EC-Council, MSAB we work closely with industry experts to ensure we are providing practical courses that give students the skills they need to enter the job market and hone skills that will set them up for the future. Possible career paths for students include forensic computer analyst, information/infrastructure security analyst, security architect, network security engineer and security systems administrator to name just a few.

It is also integral that students get the chance to learn in real-life settings. For example, our London Campus operates from the same space as the London Office for Rapid Cybersecurity Advancement (LORCA), a government-backed program that acts as a launch pad for cyber-companies through innovation and a commercialisation consultancy. By allowing our students to learn alongside leaders in the space, they're inspired to embark on a career in cyber – which is key if we're going to solve our talent issue.

At Staffordshire University London, we've also bolstered the facilities available to our students through a £3.5m into a state-of-the-art expansion. We've worked hard to ensure all our students have the facilities needed to develop the best skills for their future careers. We've just finished building a brand-new Production Warehouse, Data Junction and Digital Loft.

For example, our Data Junction is a future-thinking centre for our students with technology integrated throughout the space, including a Cisco network rack room, live cyber threat streams and wirelessly connected learning resources.

The call for people to train in cyber security is not exclusive to young people. With this increased demand for tech jobs, we need to do all we can to reskill our working population to ensure they have the skill sets. This is particularly important as a result of the pandemic.

Moving forward, we're going to need skilled individuals who can work in sectors such as cyber – and we will need people already in the workforce to retrain to be experts in these fields if we are going to have the workforce to fuel the growth of the cyber sector.

Data from the Office of National Statistics earlier this year highlights how older people, especially those over the age of 50, have been badly impacted by the pandemic, with employees aged 50 and over more likely to report working fewer hours than usual because of the pandemic between December 2020 to February 2021 compared to their younger counterparts.

As a result, we need to encourage mature students to reskill through undertaking university courses. We are not on track to achieve this, with data from the Office of Students showing a 22% decline in the number of mature students entering higher education between 2010-11 and 2018-19. We need to challenge

this status quo and normalise going to study whatever age you are if we are going to future proof our cyber sector.

As well as encouraging mature students to undertake degrees in cyber, we also need to work to ensure more gender diversity within the sector to ensure future growth. It's integral we catalyse change with Cybersecurity Ventures reporting that only 20 per cent of the global cybersecurity workforce are women. Funding continues to flow in as diversity of talents remain yet as an arduous challenge in this field.

Enhancing gender diversity within the cyber security sector in the UK is not only the right thing to do but it is integral to increasing our talent pipeline and closing the UK's cyber skills gap over the coming years.

By providing a setting where female students can flourish, universities can play a role in changing perceptions and encouraging diversity in cyber security roles. We need to provide industry-wide mentoring and coaching for women embarking on careers in the sector is required to change this stereotype.

For example, initiatives like Code First Girls are already stepping up to the plate to encourage more gender representation in STEM careers and give women a safe space to learn cyber skills. This will create a more vibrant community of cybersecurity specialists and fulfil the rapidly expanding need for cyber-attack protection.

Whilst we're doing a lot of work to future-proof the talent pipeline into the cyber by encouraging mature students and more diversity within the sector more still can be done. We need to continue to review the pipeline of cyber talent in London and ensure the capital is getting necessary investment and cyber experts to fulfil its growing needs.

As more and more start-ups, FinTechs and online businesses are headquartered in London, we will continue to need a greater pool of cyber security talent to offset the sophisticated threats in the space. It's important we continue to keep up momentum when it comes to ensuring people have the right digital skills, which is a priority for us at Staffordshire University London. ■

ABOUT THE AUTHOR

Dr Vahid Heydari Fami Tafreshi is Computing Courses (Computer Science, Cybersecurity, AI, Data Science) Provision Manager at Staffordshire University London (SUL). He has been involved with several UK/European research projects including SASH-NET (Airbus Group) and CURLING. His previous research collaborations, funded research projects and published papers that reflect his findings can be found in high-profile publications like Elsevier, IEEE & ZTE. His current research interests include Internet Protocols & Architectures, Cyber/Network Security, and Internet of Things (IoT) Security.

He received the BSc (Hons) degree in Computer Software Engineering from Shomal University, Amol, Iran, in 2007, the MSc degree in Internet Computing from University of Surrey, Guildford, in 2010, and the PhD in Electronic Engineering (Network Security) from University of Surrey, in 2015. He was a Research Fellow with the Centre for Communication Systems Research (CCSR), now Institute for Communication Systems (ICS) & home of 6G Innovation Centre (6GIC), University of Surrey. After that, he was appointed Cybersecurity & Networks Senior Lecturer within the School of Computing and Digital Technologies (CDT), Staffordshire University, Stoke-on-Trent.