

## The recruitment wall in cyber security

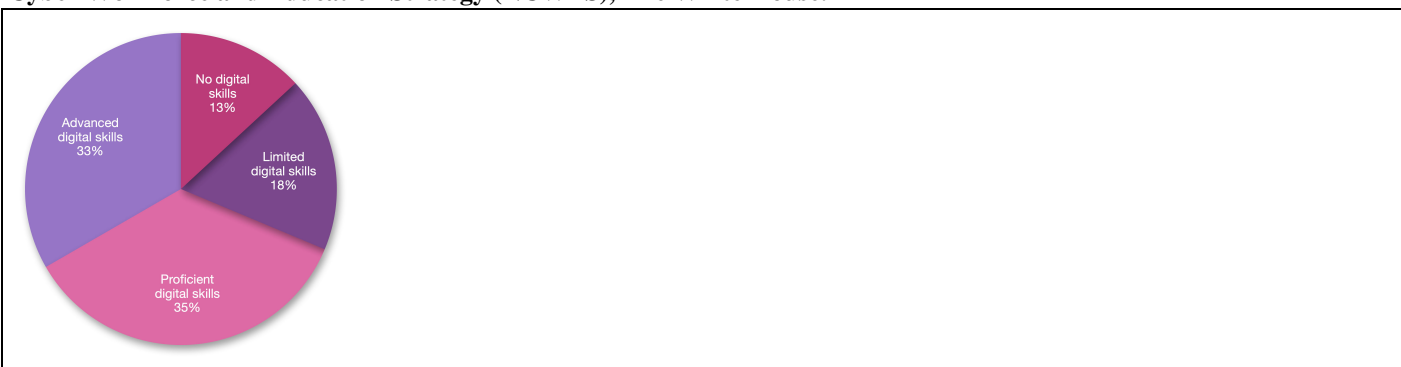
JAMAL ELMELLAS  
*Focus-on-Security*

**Abstract:** Organisations have been complaining for years about the cyber security skills gap, and the problem seems to be getting worse. However, many of the issues stem not from a lack of willing people but arbitrary barriers being placed in the way of those who would like to enter the field. We need more entry-level routes into cyber security, greater diversity and better support for training programmes.

Initiatives such as the National Cyber Strategy in the UK and the National Cyber Workforce and Education Strategy (NCWES) in the US are seeking to solve the cyber security skills gap by increasing the talent coming through the pipeline.<sup>1,2</sup> The idea is to educate the workforce of tomorrow and thereby swell the ranks.

But there are some real issues with this strategy. From the lack of entry-level openings to the rate of cumulative growth, to the fact that most entry-level personnel will be retiring in the next 20 years, all indications are that we will fail to meet demand because we're simply being too selective.

**Figure: Nearly a third of the US workforce lacks essential digital skills, let alone cyber security abilities. Source: National Cyber Workforce and Education Strategy (NCWES), The White House.**



In the UK alone, the workforce gap rose almost 30% last year, resulting in 73,439 unfilled vacancies, making it the country with the biggest gap in Europe. Worldwide, the gap is almost equal to those employed in the industry (4 million versus 5.5 million), according to the ISC2 ‘Cyber security ‘Workforce Study 2023’.<sup>3</sup>

But regardless of which route those new entrants take, be it a sideways move from an IT-related job, self-study or the more traditional academic route, those trying to enter the profession are finding it far from easy to do so due to old-school hiring practices and a culture of gatekeeping.

### Where's the gap?

One of the main problems is that the gap sees a concentration of demand in senior roles. The number of non-entry – ie, experienced – positions actually outnumbers the number of entry-level positions by two to one, found ISACA, which led the industry body to declare that there are “aspiring cyber security professionals who [have] spent significant time and money completing pathway programs and yet remain unable to secure employment in the cyber security field”.<sup>4</sup>

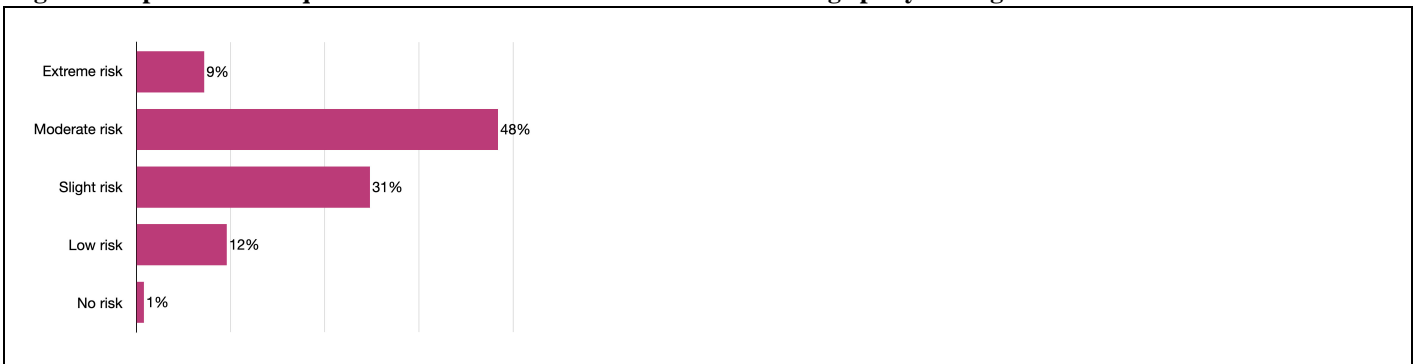
**Figure: Percentage of organisations not confident about performing basic cyber security tasks, by sector. Source: ‘ Cyber security skills in the UK labour market 2023’, Department for Science, Innovation and Technology.**



This news will undoubtedly come as a blow to those governments that have invested substantially in these programmes. In the US, there's the National Initiative for Cybersecurity Education (NICE) from NIST, which was revised in 2020 to make it relevant to those outside the federal sector.<sup>5</sup> In the UK, we've seen the launch of the Cyber Career Framework, overseen by the UK Cyber Security Council, which is continuing to map core skills to specific job titles and is expected to be completed next year.<sup>6</sup> And in the EU, we saw the European Cyber security Skills Framework (ECSF) rolled out by ENISA in late 2022.<sup>7</sup> All aim to make it easier for employers, recruiters and candidates alike to plan their workforce, inform selection, or progress their career but without the entry-level positions for them to go into, the frameworks lose their relevance.

ISACA further makes the point that the lack of entry-level positions leaves students and career-changers alike “unable to obtain employment due to lack of experience, despite any knowledge, skills or credentials they have acquired”. In short, experience trumps all other cards in their hand, with the ‘State of Cybersecurity 2023’ report revealing that hands-on cyber security experience was the primary factor for 72% when deciding if a candidate was suitably qualified.

**Figure: Responses to the question. ‘To what extent does the skills shortage put your organisation at risk?’. Source: ISC2.**



### Experience as a trump card

Using experience as a yardstick is undoubtedly exacerbating the skills gap, as it makes it harder to find candidates and fill roles. The government report ‘Cybersecurity skills in the UK labour market 2023’ found the majority of job postings (59%) request between two to six years’ experience, with those requesting three to five years’ experience proving the hardest to fill and staying open the longest.<sup>8</sup> It reports that while employers recognise that recruiting at entry level could help ease skills shortages, “this approach was regarded as challenging because of the time and cost involved and some employers only wanted to hire more-experienced candidates”.

In fact, senior-level experience was even preferred over a doctorate degree (86% vs 14%) and entry-level cyber security experience over a cyber security bachelor's degree (70% vs 30%), according to the ISC2 study, which reveals that these long-prized qualifications no longer hold the weight they once did (in part due to degree syllabuses no longer imparting the skills employers are looking for, according to ISACA).

Figure: Among organisations that identified a cyber security skills gaps, where do these gaps exist? Source: ISC2.



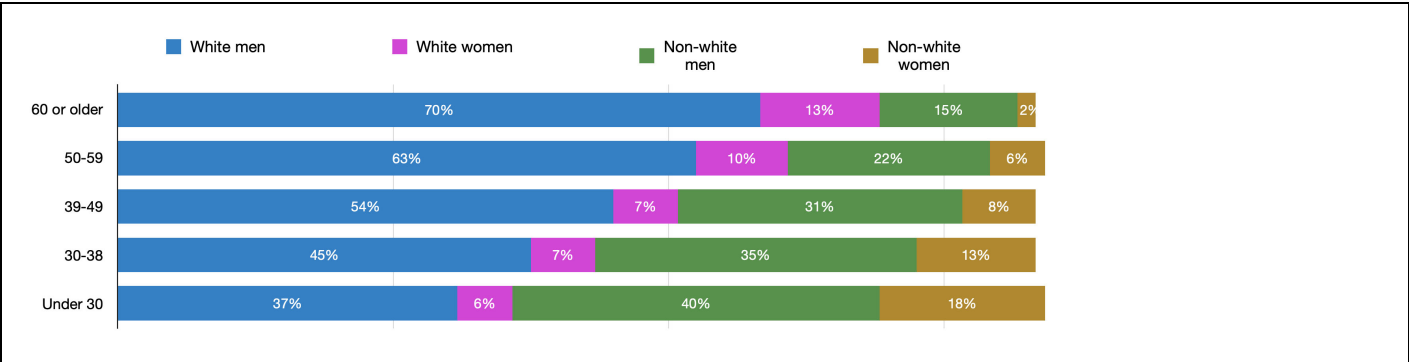
Only just under a third of those working in the profession now hold a bachelor's degree in cyber security. This is good news in some respects – ISACA has openly declared that degrees should not be mandatory for entry-level positions. But it also leaves those who want to get into the sector unsure of the best means of doing so if they can't get the necessary experience.

The ISC2 study reveals that almost 60% of hirers are seeing an increase in applications from technical personnel with no previous cyber security experience but only 51% are willing to recruit from non-cyber-security backgrounds. What this means is that the selection criteria is now out of step with market conditions and that organisations remain reluctant to broaden their hiring scope, making the process unnecessarily restrictive. There are plenty of candidates with the aptitude but not the experience who are then ruled out of the selection process. But there are even those who take a look at the job postings and then elect to take themselves out of the running because they don't view themselves as having the necessary criteria and cannot see a way to enter the fray.

**Diversity lip service**

According to the ISC2 survey, the cyber security industry is still a predominantly white male enclave, with only 18% of the global workforce female and 38% non-white. Both groups are more likely to take an education pathway than try to switch career from an IT background, which means they are doubly disadvantaged because they've chosen a traditional route and also lack experience. In the UK, the Government report found that diversity hiring seems to have at best stalled and at worst gone into decline. Those placed from ethnic backgrounds went from 25% to 22% last year and female placements dropped from 22% to 17%.

Figure: Breakdown of cyber security staff. Source: ISC2.



Diversity, equity and inclusion (DEI) initiatives are slowly being adopted but only 40% use skills-based hiring – that is, evaluating talent based on skills and potential – according to the ISC2. Shockingly a fifth of all of those questioned, irrespective of gender or race, said they felt discriminated against, which is not helped by the fact that only 42% had anonymous discriminatory reporting processes in place. Failing to provide these support mechanisms can see discrimination continue to persist and ultimately result in staff attrition, so it's just as important for organisations to focus on a positive company culture as well as invest in DEI recruitment.

### Upskilling

Of course, candidates can improve their chances of selection through upskilling and determining which skills are in high demand to shift the balance in their favour. The skills gap differs markedly from the workforce gap, with the former referring to skills in short supply while the latter is the headcount needed to meet demand overall. The two are not the same and, from the organisation's point of view, it is possible to reduce the workforce shortage by ensuring that the skills you need are represented within the team. Concentrating on addressing the skills gap can therefore work in both the hirer and the candidate's favour.

The top skills in demand were found to be identity and access management (IAM), cloud security and data protection, according to the ISACA study, but among those with less than three years' experience it was security controls – ie, endpoint, network and application security – which topped the league. However, soft skills were also in demand, potentially allowing new entrants to gain the advantage, with communication, critical thinking, problem solving and teamwork all scoring highly.

There is also much debate over whether skills in artificial intelligence will become key. The majority (84%) of cyber professionals admit they have no or minimal knowledge or only some or moderate knowledge of AI and machine learning, found ISC2, again allowing those coming into the sector to steal a march.

However, candidate self-study and government pathways can only get us so far. Ultimately it comes down to the commercial sector to make entry-level placements available and to provide the training to allow those lacking experience to get up to speed.

### Don't terminate training

As a sector renowned for its support of lifelong learning in the form of vendor and non-vendor certification programmes, the basis for this learning is already in place. However, support for these programmes is now being withdrawn in the face of economic austerity.

ISC2 found that 35% of organisations have eliminated their cyber security training programmes. Moreover, almost half (47%) no longer offer reimbursement for certification courses or exams and ISACA found that those offering tuition reimbursement had fallen to just 20%. Such a tactic that might result in short-term gains but long term will almost certainly harm the ability of the organisation to attract and retain staff, or to keep pace with technological change and the evolving threat spectrum.

At the present time, most organisations are attempting to deal with the skills crisis through enabling staff to cross over into security roles (45%), outsourcing (38%) and reskilling (21%), according to ISACA. Only 20% are offering performance-based training and only 19% apprenticeships or internships. But without hiring and training these non-experienced personnel, we will never be able to satisfy the demand for middle- and senior-level cyber security personnel.

It's worth bearing in mind also that ISC2 found most new entrants (48%) are aged 39 years or older, having switched careers so will be retiring sooner, creating a superficial balloon of supply that will not really satisfy demand.

### A new mindset

Going forward, we need to encourage new entrants from all walks of life and all ages to apply, and seek to provide them with the opportunities to grow and build up their experience. But doing so will require hirers to carry out evaluations based on soft skills that focus on potential not on experience and to change their mindset when it comes to the value of roles.

As a sector, there's always been a tendency to perceive those with technical expertise as having more value because they can understand the tooling and coding. But the need for that depth of knowledge is diminishing as no-code gains ground, AI augments jobs and security is democratised in the business. So will we need a developer's level of understanding or will security skills move more towards analysis and problem solving? Only time will tell.

It's been said before but is worth reiterating that to many in the business there is no workforce gap. That's because there are plenty of potential candidates out there to fill those roles. What's stopping us from is our own bias and willingness to equip them to do the job.

### About the author

*Jamal Elmellas is chief operating officer at Focus on Security ([www.focuscloudgroup.org](http://www.focuscloudgroup.org)), 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.*

**Figure: Jamal Elmellas, Focus-on-Security**



**References:**

1. 'National Cyber Strategy 2022'. Cabinet Office, 15 Dec 2021. Accessed Apr 2024. [www.gov.uk/government/publications/national-cyber-strategy-2022](http://www.gov.uk/government/publications/national-cyber-strategy-2022).
2. 'National Cyber Workforce and Education Strategy'. The White House, 31 Jul 2023. Accessed Apr 2024. [www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf](http://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf).
3. 'ISC2 Cyber security Workforce Study 2023', ISC2, Oct 2023. Accessed 26 Feb 2023. [www.isc2.org/research](http://www.isc2.org/research).
4. 'State of Cyber security 2023', ISACA, 2 Oct 2023. Accessed 26 Feb 2024. [www.isaca.org/state-of-cybersecurity-2023](http://www.isaca.org/state-of-cybersecurity-2023).
5. 'National Initiative for Cyber security Education (NICE)', NIST. Accessed 26 Feb 2024. [www.nist.gov/itl/applied-cybersecurity/nice](http://www.nist.gov/itl/applied-cybersecurity/nice).
6. 'Cyber Career Framework', UK Cyber Security Council. Accessed 26 Feb 2024. [www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/](http://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/).
7. 'European Cyber security Skills Framework (ECSF)', ENISA, Sep 2022. Accessed 26 Feb 2024. [www.enisa.europa.eu/topics/education/european-cyber-security-skills-framework](http://www.enisa.europa.eu/topics/education/european-cyber-security-skills-framework).
8. 'Cyber security skills in the UK labour market 2023'. Department for Science, Innovation and Technology, 24 Jul 2023. Accessed 26 Feb 2024. [https://assets.publishing.service.gov.uk/media/64be95f0d4051a00145a91ec/Cyber\\_security\\_skills\\_in\\_the\\_UK\\_labour\\_market\\_2023.pdf](https://assets.publishing.service.gov.uk/media/64be95f0d4051a00145a91ec/Cyber_security_skills_in_the_UK_labour_market_2023.pdf)