Cyber Security Recruitment Report

The Department for Culture, Media and Sport published **Understanding the Cyber Security Recruitment Pool research report**, which quantifies and explores the supply of cyber skills in the UK. It covers:

- The size and geographic location of the recruitment pool
- The types of skills and experience that are prevalent in the pool
- Recommendations on how employers can effectively recruit from the pool

The below summary of the report is provided by Dods. From page 5 the Cyber Security Labour Market Report is summarised.

Key findings

Quantitative research findings:

- The current UK cyber security workforce currently has an estimated 98,000 (low) – 171,000 (high) employees. We take the mid-point for modelling purposes (i.e. 134,500 individuals);
- The demand for cyber security professionals has grown by an average of 14 percent per annum since 2016. In the most recent year, it has grown by nine percent. This implies that the UK cyber security workforce would need to grow by approximately 12,000 people per annum (to meet expected demand). However, we do recognise that this assumes a direct relationship between demand and employment (which may be partially affected by processes such as automation and labour costs);
- The cyber security workforce is also losing approximately four percent of staff each year to retirement or exiting to other sectors. We estimate that this consists of approximately 4,000 – 7,000 (mid-point of 5,500) people each year;
- In total, this implies that the UK cyber security workforce needs to attract at least 17,500 people each year to meet both new demand and replace lost workers. This broadly aligns with the Cyber Skills in the UK Labour Market research, which indicates there were over 33,000 online job vacancies posted by employers in the UK seeking core cyber security talent in 2020.
- With respect to inflows, we estimate that there are approximately 7,500 new individuals entering into a cyber security career each year. This includes approximately 4,000 UK university graduates (undergraduate and postgraduate level) entering employment in cyber security roles, up to 2,500 undertaking career conversion, re-training, or entering the UK pool elsewhere, and up to 1,000 involved in apprenticeships in cyber security. This figure could be increased in the future through retraining initiatives, support with certifications and skills, and potentially expansion of the volume enrolled in higher and further education courses;
- This implies that the UK should be attracting c. 17,500 new people each year into cyber security employment to meet demand but is currently only generating c. 7,500 in new supply. **This suggests an annual shortfall (2021) of c. 10,000 people**, and this is in addition to existing perceived shortage of talent currently, as well as potential for further demand to increase in future. This highlights that the cyber skills shortage is an ongoing challenge that needs to be addressed rapidly in order to mitigate some of the resulting issues (e.g. loss of talent and experience, challenges in staff retention and productivity, risk of staff burnout etc.);

- This also suggests that, left untreated, the extent of the shortfall will continue to worsen, as cyber security remains an area where demand for talent exceeds supply; and
- However, we do consider the use of regional, national, and online re-skilling initiatives – if scaled, could considerably tackle this shortfall with sufficient funding and support. Further, these initiatives are often also useful in tackling barriers to entering the cyber security field (e.g. through provision of initiatives targeted to those with neurodiversity, those under-represented in the industry e.g. women, and those from ethnic minority backgrounds, and promoting cyber as a career to those previously in aligned pathways e.g. military and law enforcement).

Qualitative research findings:

They also undertook qualitative research with 25 stakeholders. These included cyber security employers, training providers, recruitment agents and employees.

- Employers stated they were struggling to fill roles, especially specialist roles for employees with 3-5 years experiences. However, training providers and recruitment agents believed the level of demand for courses and roles are high. This implied that there are not enough suitable candidates in the pool. A low indicative ratio of high-quality applicants being seen as suitable to their role further backed this up.
- Other stakeholders felt that there was sufficient quantity in the pool. Some consultees felt that employers were trying too hard to find the perfect candidate. They mentioned that there were entry-level candidates in the pool from other areas, such as the military. These groups had a strong set of soft skills, such as leadership, project and communication skills. They felt they were able to learn technical skills via on the job training. Consultees suggested the government could help increase quantity and quality by increasing education and information on cyber security in schools.
- There was also a lack of diversity in the pool. Recruitment and interview processes, unsuitable working environments and inaccessible training made it difficult for neurodiverse candidates to enter the pool, and once in it, find a role. There are specialist training providers attempting to alleviate this. However, government can help alleviate this by facilitating relationships between training providers, autism charities and employers, and by setting an example themselves in how to improve neurodiversity in the workplace.
- Women were under-represented at all levels in the pool, with ethnic minority candidates less successful in getting roles at leadership level. At senior levels, blind recruitment and transparent promotion processes could help alleviate this, with positions currently heavily reliant on networking. Consultees felt the government could advise employers on this, as well as lead the way in making them adhere to standards if bidding for government contracts. There was also a perception issue amongst women who could potentially enter the pool. Consultees felt the government can help alleviate this by helping educational institutions make it clear what a career in cyber truly entails.
- Those with lower educational qualifications were also under-represented, with suitable candidates tending to be educated to degree level. Government could help by improving and increasing further education courses and apprenticeships.
- Despite concerns about diversity and getting candidates with strong complimentary skills into roles, there was broad agreement that there is a low level of technical expertise relative to demand. This was evidenced by employers stating that specialist roles such as penetration testers or firewall engineers

were most difficult to fill. Internal on the job training by employers for individuals with strong complementary skills and encouraging employees to seek external accreditation could help alleviate this in the short term. In the long term more bespoke FE courses and apprenticeships are required.

- Overall, there was a sense that the future of the recruitment pool is positive and that current government interventions, such as CyberFirst, are working. They felt that the increase in digital employment has made training more accessible, and will broaden the pool both in terms of raw numbers, and the wider diversity of the pool. They felt that successful education interventions and reskilling would mean candidates come from a greater range of educational pathways, and that remote working would help improve the working environment for women.
- The coronavirus pandemic further provides an opportunity. There was a sense that it could be used as a catalyst for the government to increase their role in reskilling the wider workforce in cyber security. This could be used to help those who are unemployed or furloughed because of the pandemic, with a perception amongst new entrants that cyber security offers stable employment.

Recommendations

Theme 1: Boosting the supply of new talent, and recognising the role of cyber security roles in driving economic recovery

- This research highlights that the traditional cyber recruitment pool (e.g. graduates and experienced staff) is much smaller than some employers might recognise. In order to address the shortage of cyber security talent, we recommend that alternative and innovative routes to a cyber security career need to be clear, funded and accelerated. These should also be targeted to a diverse range of individuals.
- The economic impact of the COVID-19 pandemic has demonstrated the critical role of retraining and upskilling. The current economic conditions mean that there is much greater demand for engaging in retraining initiatives, particularly among individuals that have faced redundancy or reduced hours of working in existing roles. There is a window of opportunity for the UK to rapidly invest in cyber security retraining initiatives, courses, and learning models to increase future productivity.
- Leading by example. Throughout this research, we note several examples of good practice in increasing the supply of new talent into the cyber security industry. We recommend further activity should be undertaken to better promote the understanding and take-up of such initiatives. This could include greater public sector uptake of such schemes (including retraining) where possible, and the sustained promotion of ‘what works’ across industry.

Theme 2: Supporting pathways into cyber security employment

- Time to scale up. As noted, there are several pilot and early-stage initiatives that appear to have gained traction in improving diversity and access to cyber security training and entry-level employment. There is now a strong mix of examples across further and higher education, private training initiatives, bootcamps, employer-led training models, and academies targeted at retraining particular groups such as neurodiverse and former Armed Forces. We recommend that further support to help successful pilot initiatives scale-up faster (and to do so across the UK) would be particularly welcome given the identification of the current cyber security skills gaps.
- We further recommend that in addition to supporting supply-based initiatives, government and training providers should work closely with industry at a regional level to help match skills with local demand. For example, these models should ideally have a clear outcome whereby those supported can enter a

role with a local employer in need of such skills. We note that this should also be considered as an important component of the Levelling Up Agenda, as the type of demand for cyber security professionals can vary across the UK, and there is significant potential to increase regional productivity given the longer term salary premium associated with cyber security roles.

- The nature of cyber security roles has expanded in recent years. We recommend that addressing the cyber security recruitment gap will also require providing and supporting other digital skills pathways, and supporting individuals move into highly complementary roles such as Governance, Risk and Compliance roles. In this respect, improved segmentation, and definition of what skills (including less technical') and type of 'cyber security career' an individual could have may help to ease some of the shortage, and better improve allocation of resources.

Theme 3: Undertaking workforce planning to meet the needs of the cyber security industry today, and into the future

- We recommend that government further explores a Capacity Review of Higher Education Institutions (HEIs) in the UK with respect to cyber security provision. Whilst this study has explored the number of students graduating within 'Cyber Security' and Computer Science courses, a capacity review of undergraduate and postgraduate cyber provision may be useful to understand if and how HEIs may be able to increase supply (if at all, and without impacting quality) of cyber security teaching, and to further understand the prevalence of cyber security modules across all degree pathways.

- Building on this theme, we would also recommend that a 'workforce planning' approach should be explored at regional and national levels, particularly by Local Enterprise Partnerships (LEPs) and devolved equivalents. This research has estimated a UK based shortfall in the number of new entrants to the recruitment pool. However, this availability of supply will vary regionally, as will employer demand. Improving alignment between regional skills supply and employer demand, and understanding regional growth ambitions should help regions to make informed decisions and investments to support retraining.

Theme 4: A strong focus on improving diversity in supply

The Cyber Skills in the UK Labour Market (2021) explores themes of diversity within the cyber security labour market. However, the following recommendations are included below:

- Retraining initiatives to support individuals get into cyber security can be life changing. They can allow people to learn new skills, meet new people, and increase their earning power. However, we recommend that such initiatives should place a sustained emphasis where possible, on improving accessibility to all extents. Whilst many individuals may want to retrain, the barriers to undertaking such initiatives such be continually explored. For example, this might include provision of financial support (e.g. direct, or support with child-care) to enable the take-up of the training place.

- As set out in the research, whilst there have been a number of initiatives aimed at improving diversity within the industry, there are still significant issues reflected in the inflows of new talent (e.g. female take-up of cyber security courses remains low). We recommend that these figures are closely monitored in future years, alongside the continued promotion of schemes such as CyberFirst.

Cyber Security Labour Market Report

DCMS published the **Cyber Security Skills in the UK Labour Market 2021 report**, which explores the nature and extent of cyber security skills gaps (people lacking appropriate skills), skills shortages (a lack of people available to work in cyber security job roles) and job vacancies in the UK.

The research uses a mixture of:

Representative surveys with cyber sector businesses and the wider population of UK organisations (businesses, charities and public sector organisations – with a focus on businesses)

- Qualitative research with training providers, cyber firms and large organisations in various sectors
- A secondary analysis of cyber security job postings using the Burning Glass Technologies database.

Key findings

Skills gaps:

- Approximately 680,000 businesses (50%) have a basic skills gap. That is, the people in charge of cyber security in those businesses lack the confidence to carry out the kinds of basic tasks laid out in the government-endorsed Cyber Essentials scheme, and are not getting support from external cyber security providers. The most common of these skills gaps are in storing or transferring personal data, setting up configured firewalls, and detecting and removing malware
- Approximately 449,000 businesses (33%) have more advanced skills gaps, most commonly in areas such as penetration testing, forensic analysis and security architecture
- A third (32%) have a skills gap when it comes to incident response (and do not outsource this)
- Almost half (47%) of cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants. A total of 13 per cent say that job applicants having these skills gaps has prevented them from achieving business goals to a great extent
- Technical skills gaps were most commonly cited in the following 3 areas: incident management, investigation and digital forensics (41% of the firms identifying any technical skills gaps), assurance, audits, compliance and testing (37%) and cyber security research (36%)
- Around 1 in 5 cyber firms (18%) also say that job applicants lacking non-technical skills, such as communication, leadership or management skills, have prevented them from meeting their business goals. Around a quarter (23%) say this about their existing employees

Qualifications and training:

- 8 in 10 cyber firms (79%) have provided training for staff in cyber roles in the last 12 months, whereas around quarter (23%) of businesses outside the cyber sector have done so
- 7 in 10 cyber firms (70%) report employing staff who have, or are working towards, cyber securityrelated qualifications (i.e. in higher education, apprenticeships or other certified training)
- Consistent with the previous 3 years, the most commonly requested certification by cyber employers is Certified Information Systems Security Professional (CISSP), which is in 36 per cent of online job

postings that ask for a specific certification. Cisco Certified Network certifications are also in high demand, with 23 per cent requesting Cisco Certified Network Professionals (CCNP)

- Large cyber firms often had structured career development programmes, which were felt to help with staff retention. Smaller firms relied much more on on-the-job training, work shadowing, mentoring schemes and self-directed learning
- Interviewees highlighted ongoing training gaps in terms of building soft skills, such as presenting and proposal writing skills. Their other major training needs were typically in niche technical areas related to their products or services, where it was sometimes hard to find focused training

Recruitment and staff retention:

- The most common reason given for this continues to be around candidates lacking technical skills or knowledge (48% of employers with hard-to-fill vacancies), but mentions of job applicants lacking work experience have increased since the previous study (from 8% to 35%)
- In 3 in 10 cases (30%), cyber firms have found it hard to fill generalist roles (where employees are expected to work in a range of cyber security areas). The most common shortages in specialist roles are for senior management roles, penetration testing and security architecture
- The most common roles in demand are security engineers (34%), security analysts (18%), security managers (14%), security architects (11%) and security consultants (7%)
- The sectors most in demand of cyber talent are the consultancy, finance and insurance, IT and cyber security sectors
- The technical skills areas most in demand are very consistent with the previous 3 years, and include skills around network engineering, risk management and technical controls, operating systems and virtualisation, cryptography and programming
- There are still geographic hotspots where demand is strongest, in cities like London, Leeds, Edinburgh, and Belfast, and across the West Midlands and the South West (in Bristol, Cheltenham and wider Gloucestershire)
- Across cyber sector firms, a total of 6 per cent of the cyber workforce are estimated to have left their posts since the start of 2019, with 4 per cent leaving of their own volition. Employers most commonly attribute this to a lack of pay or benefits. However, outside the cyber sector, the qualitative interviews highlight that a poor cyber security culture can also frequently drive people to leave cyber roles and look elsewhere.

Diversity:

- 17 per cent of the workforce come from ethnic minority backgrounds, falling to just 3 per cent of those in senior cyber roles (i.e. those typically requiring 6 or more years of experience)
- 16 per cent are female (vs. 28% across all digital sectors), falling to 3 per cent in senior roles
- 10 per cent are neurodivergent, falling to 2 per cent in senior roles
- 9 per cent are physically disabled, falling to 1 per cent in senior roles

- Employers saw the lack of diversity among their own workforces as resulting primarily from a lack of applications from diverse groups. On the other hand, some recruitment agents felt that the hiring managers for cyber roles needed more educating on unconscious bias, best practice in writing unbiased job profiles and concepts such as blind recruitment
- The ongoing preference for recruiting via personal networks and word-of-mouth recommendations, particularly for senior roles, may have implications for diversity. Interviewees acknowledged that it can lead to employers accessing the same, narrow recruitment pools

The impact of Covid-19:

- Outside the cyber sector, COVID-19 had often brought cyber security to the fore, as organisations had to rapidly shift to a remote working environment whilst still maintaining service continuity. This shift typically increased workloads and put more pressure on cyber teams, but also presented opportunities to engage board members, and argue for extra investment in training and personnel
- Organisations had been forced to make all their cyber security training virtual. This raised challenges around replicating classroom environments online. Shadowing on the job was also seen to be harder in a virtual environment
- Employers and recruitment agents expected there to be a bigger cyber security talent pool available, at least temporarily, due to job losses in sectors negatively impacted by COVID-19
- Recruitment was expected to become more geographically diverse, with more candidates applying from further afield thanks to remote working. There is some evidence for this from the job vacancies analysis, with a slight fall in the proportion of job vacancies that were in London, and some small increases in the North West, Northern Ireland and the East Midlands

Changes over time:

- Businesses are less likely to report a range of basic skills gaps than in the 2018 study, in areas like firewall configuration, restricting software and admin rights, secure configurations and patching
- Cyber leads across businesses are more likely to think that their senior managers understand the cyber security risks their organisation faces (up from 62% in 2018 to 77% this year)
- Fewer cyber sector firms report technical skills gaps than in 2020, both among existing employees and among job applicants (down from 64% to 47%)
- More cyber sector firms have undertaken a training needs analysis than in the 2020 study (up from 49% to 60%) and more have provided training for staff in cyber roles (up from 73% to 79%)
- More cyber sector firms report having at least one employee with, or working towards, a cyber security-related qualification or certification (up from 62% to 70%)

Recommendations

Changing attitudes and behaviours:

- The existing NCSC guidance for communicating cyber security risks to board members should be reviewed and, if necessary, updated and further promoted to ensure it helps cyber leads frame discussions in terms of commercial risk.

- There should be further guidance (e.g. on awareness raising and training activities), access to best practice and solutions for cyber leads on what works to change and maintain the behaviour of wider staff (outside of cyber teams) when it comes to cyber security.
- The ability to positively influence the behaviour and culture within organisations should be included as part of the overall skills requirement for any Chartered Cyber Professional. These skills should also be included in the Qualifications Framework to be developed by the UK Cyber Security Council.

Career pathways and transitions:

- The ongoing work to map cyber security career pathways should include the development of example job descriptions and suggested minimum qualifications requirements for typical roles, to encourage cyber employers to draft more realistic job adverts.
- The upcoming Career Pathways Framework for cyber security should include a set of training pathways or other innovative solutions that can quickly enable staff in a range of IT roles to gain essential cyber security skills or transition into cyber specialist roles. These solutions should be rolled out and promoted as soon as possible, potentially ahead of the overall Framework.

Recruitment and workforce diversity:

- Smaller businesses in the cyber sector should be encouraged and supported to build relationships with schools, colleges and universities in order to run work placements and internships, for example through a dedicated website or exchange scheme. This should enable them to take on more entry-level staff in cyber roles and carry out recruitment beyond their existing networks.
- There should be written guidance or training materials targeted at cyber leads from small organisations – especially those that lack HR support – informing them of the basic actions they could take to improve diversity. This includes, for example, things like writing neutral job adverts and making working environments suitable for neurodivergent employees.
- Recruitment agents and HR staff should play a bigger role in educating cyber leads on good practice for realistic and unbiased recruitment. This might include, for example, events or workshops at cyber security conferences led by recruitment agents or HR professionals.
- There should be further work to understand the reasons behind the lack of diversity in senior roles within cyber sector firms – an issue which potentially extends into senior cyber roles outside the sector – and the steps that would improve career progression into these senior roles for diverse groups.