Cyber security skills in the UK labour market 2023

Findings report

Steve Coutinho, Alex Bollen, Claire Weil, Chloe Sheerin, Dejon Silvera, Ipsos
Sam Donaldson, Jade Rosborough, Perspective Economics

Department for Science, Innovation & Technology

Ipsos

Contents

Summary

This is a summary of research into the UK cyber security labour market, carried out on behalf of the Department for Science, Innovation and Technology (DSIT). In February 2023, the parts of the then-Department for Digital, Culture, Media and Sport (DCMS) responsible for cyber security policy moved to DSIT.

The research explores the nature and extent of cyber security skills gaps (people lacking appropriate skills) and skills shortages (a lack of people available to work in cyber security job roles) using a mixture of:

- Representative surveys of cyber sector businesses and the wider population of UK organisations (businesses, charities and public sector organisations – with this summary focusing mainly on businesses)
- Qualitative research with recruitment agents, cyber firms and medium/large organisations in various sectors
- A secondary analysis of cyber security job postings on the Lightcast labour market database, as well as recruitment pool data originating from the Higher Education Statistics Authority (HESA) and Jisc

This is the fifth iteration of the research, which has been carried out on an670 annual basis.

Skills gaps

A high proportion of UK businesses continue to lack staff with the technical skills, incident response skills and governance skills needed to manage their cyber security. We estimate that:

- Approximately 739,000 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 setting up configured firewalls, storing or transferring personal data, and detecting and removing malware
- Approximately 487,000 businesses (33%) have more advanced skills gaps, most commonly in forensic analysis of breaches, security architecture, interpreting malicious code and penetration testing
- 41% have an internal skills gap when it comes to incident response and recovery, and do not have this aspect of cyber security resourced externally

The figures for basic and advanced technical skills gaps have not changed significantly across the 5 years of data. However, the proportion of businesses lacking confidence in incident management skills is trending upwards over time (27% in 2020, 32% in 2021, 37% in 2022 and 41% now).

The qualitative evidence continues to suggest, as we have found in previous years, that some cyber leads can struggle to engage senior leadership with cyber security at all. For other cyber leads, the issue was more that senior leadership acknowledged the importance of cyber security but did not necessarily prioritise it as much as they would have liked. A lack of resources was also a constraint. Cyber leads said they could feel pressurised and pulled in different directions. Some had to perform other roles on top of their cyber security responsibilities.

In the quantitative research, 84% of staff in the private sector carrying out any cyber functions have absorbed these tasks into an existing role. In contrast, in the cyber sector 47% have previously worked in a cyber role elsewhere.

Nevertheless, skills gaps are also common in the cyber sector:

- 49% of all cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants
- 22% of cyber sector employers report having existing employees who lack necessary technical skills and 44% say that the job applicants they have seen lack necessary technical skills
- Technical skills gaps were most often cited in these 3 areas: security testing (35%), cyber security governance and risk management (31%) and secure system architecture and design (30%)

The number of cyber firms experiencing complementary skills gaps continues to be almost as high as the proportion with technical skills gaps. 43% have experienced a complementary skills gap in the previous 12 months, with either job applicants or existing employees being seen to lack skills in areas such as communication, leadership, management, or sales and marketing. This is in line with last year (when it was 41%).

Cyber Specialisms and the UK Cyber Security Career Route Map:

This year was the first year of the study that included a survey question which focused on the 16 specialisms outlined in the UK Cyber Security Career Route Map, to make it easier for individuals to enter cyber security roles via a range of possible pathways. The UK Cyber Security Career Route Map has been renamed by the UK Cyber Security Council to “The Cyber Career Framework.” However, since this was the name that was referred to throughout survey fieldwork and in all qualitative interviews we will continue to refer to it as the UK Cyber Security Career Route Map throughout the report. According to these new statistics:

- The highest prevalence among the 16 specialisms included was found in cyber security generalists, with 61% of cyber sector firms having employees working in this role. The highest prevalence among the 16 specialisms included was found in cyber security generalists, with 61% of cyber sector firms having employees working in this role. Despite this high prevalence, results from the 2022 survey found that generalists comprised 26% of the cyber security workforce. In the 2023 survey the definition outlined in the UK Cyber Security Career Route Map of a Cyber Security Generalist was “the performance of the duties of multiple cyber security specialisms in one role.” Respondents were also instructed to select Cyber Security Generalist if they felt the work they did was equally spread across the specialisms listed in the Careers Route Map.
- Beyond these generalists, the distribution of cyber security roles in the sector is not skewed towards one specialism. After cyber security generalists, 40% of cyber sector firms have employees in cyber security management or audit and assurance. Digital forensics and cryptography/communications security have the lowest proportion but there is a relatively even spread across the 16 specialisms

In the qualitative research, reaction to the Route Map was generally positive. We found that:

- Most employers and recruiters taking part in the qualitative research had not heard of the Careers Route Map. A few of those who were aware of the Route Map had used it or had contemplated doing so for training and standardising cyber roles
- Employers and recruiters generally felt it was useful to have individual roles and specialisms set out in the Route Map. This could help with understanding what skills there were in their organisation, potential career progression for their cyber staff, and recruitment
- A few from outside the cyber sector felt the Route Map was too specialist for their needs and some struggled to understand it

Recruitment and staff retention

The demand for cyber security professionals has continued to increase. In 2022, there were 160,035 relevant job postings, of which 71,054 job postings were across core cyber roles (an average of 5,921 per month), and 88,981 were other job postings requesting cyber security skills. When compared to 2021 levels, this suggests that the number of core cyber job postings has increased by 33% (from 53,586 in 2021). Demand for ‘all cyber roles’ has also increased by 30% in this time period.

However, there is some evidence which suggests that demand slowed in the second half of 2022. There were 37,851 core postings the first half of 2022 compared with 33,203 postings in the second half, potentially reflecting a slight slow-down in recruitment activity. Nevertheless, this demand remains high compared with historic trends.

Employment in the cyber workforce has increased by 10% within the last year. This suggests a need for 13,500 new people each year to meet demand, in addition to the c.4,700 to replace those exiting the sector, i.e. a total requirement of c.18,200 per year. A total of c.7,000 individuals entered the cyber security workforce in 2022, leaving an estimated shortfall in 2022 of c.11,200 people. This is lower than last year’s estimate of c.14,100. This is due to a smaller growth rate of the workforce (it was 13% last year). The gap remains persistent and is annually cumulative in effect.

The number of students enrolled in cyber security courses has increased by 29% (from 14,910 to 19,200) and the number of students graduating in a cyber security course has also increased by 19% (from 3,670 to 4,360). This increase is a positive step towards reducing the workforce gap.

The survey research found that 53% of cyber sector businesses have tried to recruit someone in a cyber role since the beginning of 2021. The average number of vacancies per firm has risen, standing at 5.2 in 2021, 6.8 in 2022 and 8.2 this year. 37% of cyber vacancies posted since the start of 2021 are reported as being hard to fill, which is slightly lower than the estimate from last year (44%) and in line with the year before (37%). The most common reason given for this continues to be around candidates lacking technical skills or knowledge, which is similar to findings from 2022 and 2021.

Skills shortages continue to exist in approximately equal measure in specialist and generalist roles (where candidates are expected to understand a range of cyber security areas, but not necessarily in depth). In the qualitative research, we found that employers particularly valued staff with strong technical and complementary skills but these candidates can be hard to find (‘unicorns’ was one description).

As we have found in previous years, cyber sector businesses find positions for staff with 3 to 5 years of experience the hardest to fill. This is also reflected in the job postings analysis, where 59% of postings request 2-6 years of experience.

In the qualitative research, recruiters and employers regarded salary as a key to successful recruitment. However, not all employers can offer competitive salaries to attract talent and fill hard-to-fill vacancies. Other important factors identified by employers and recruiters in attracting candidates were benefits packages, opportunities for development/training, work culture, interesting work and hybrid/remote working.

There is evidence that more employers are advertising vacancies for work that can be undertaken remotely or from home (i.e. outside the regions in which they are based). We estimate that 28% of job postings for core cyber roles had no regional location listed (i.e. the roles were marked as ‘Remote’ or ‘UK-wide’). This is an increase from 2021 (21%) and 2020 levels (13%), which suggests an embedded trend towards working from home and remote working across all regions in cyber security.

In the qualitative research, some employers said that offering hybrid or remote working enabled them to widen their talent pool and make them a more attractive proposition to candidates. However, others preferred to have staff in the office. A few found that local candidates were being siphoned off to work for organisations further afield which could offer higher salaries.

Some employers taking part in the qualitative research felt that recruiting at entry-level could be one solution to skills' shortages. However, this approach was regarded as challenging because of the time and cost involved and some employers only wanted to hire more experienced candidates.

In terms of staff leaving cyber firms, a total of 9% left of their own volition, with the remaining 1% leaving due to dismissal. This is consistent with last year’s findings. The most common reason for staff leaving was that the company offer was not good enough, overtaking last year’s top reason of better pay or benefits.

In the qualitative research, while some employers had no retention strategies as such, or were philosophical about staff leaving, others tried to retain staff by offering opportunities for progression, skills development and interesting work. However, offering training carried the risk that employees then leave because they have become more valuable in the marketplace.

Diversity

The diversity of the cyber sector workforce has remained consistent. The 2023 data shows that:

- People from ethnic minority backgrounds make up 22% of the sector workforce, similar to last year’s figure of 25%, and 14% of those in senior cyber roles are from ethnic minority backgrounds (i.e. those typically requiring 6 or more years of experience)
- 17% of the workforce are female, which is in line with our findings in 2020 and 2021. While this is a slight reduction from the previous year (22%), the change is not statistically significant Women account for 14% of those in senior roles
- 12% are neurodivergent, and this group makes up 6% of those in senior roles
- 7% are physically disabled, with 3% in senior roles

The proportion of cyber roles held by women remains lower than for other digital sectors (17% vs. 29% across all UK digital sectors). These figures again highlight an untapped recruitment pool, with the potential to transition more women into cyber roles. In contrast the figure for ethnic minorities is slightly higher than the digital workforce as a whole (22% for the cyber sector vs. 18% across all digital sectors).

In the qualitative research, some felt that there had been progress on diversity in the past few years with more women and/or ethnic minorities in the industry. This was attributed to both a leadership and industry focus on improving diversity and a greater understanding of the benefits of a more diverse workforce.

Among cyber firms who have tried to recruit people into cyber roles since January 2021 (53% of the total), 40% have taken any action to adapt their recruitment processes or carried out specific activities to encourage applications from diverse groups. In the qualitative research, employers taking steps to improve diversity in recruitment were often focusing their efforts on entry level positions. One hurdle here is that the gender gap for cyber security courses remains wide, with only 12% of female graduates at undergraduate level, and 23% at postgraduate level.

Many of the employers taking part in the qualitative research reported difficulties recruiting staff from diverse groups. As we have found in previous years, the key issue here is the candidate pool. There was uncertainty about how to go about recruiting more diverse groups and the cost of doing so was also raised as a barrier.

Greater diversity will widen the talent pool. There is a needs to encourage diverse groups into cyber careers. Initiatives such as the UK Cyber Security Council's Careers Route Map also have an important part to play in supporting individuals with transferable skills to transition into cyber roles. This is particularly the case for employers who do not have the resources to recruit and train cyber staff at entry level.

Conclusions

This report on the cyber security labour market is in line with many of the key messages from previous years. The main lessons are as follows:

- Across the economy, it is still common to find skills gaps in basic technical areas. Skills gaps around incident management are increasing over time
- Demand for cyber security professionals has risen again this year, although there are signs of a slowdown in the second half of the year
- New estimates for proportions of the workforce in the cyber sector in specific roles show a high prevalence of generalists
- Widening and increasing the talent pool remains key to tackling skills shortages and improving diversity

Introduction

1.1 About this research

The UK government Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos and Perspective Economics to conduct the latest in an annual series of studies to improve their understanding of the current UK cyber security skills labour market. In February 2023, the parts of DCMS responsible for cyber security policy moved to the new Department for Science, Innovation and Technology (DSIT). The previous studies were published by DCMS in 2022 (fieldwork in 2021), 2021 (fieldwork in 2020), 2020 (fieldwork in 2019) and 2018. [^1]

The 2023 research, in line with previous years, aimed to gather evidence on:

- Current cyber security skills gaps (i.e. where existing employees or job applicants for cyber roles lack particular skills)
- Current skills shortages and the level and type of job roles they affect (i.e. a shortfall in the number of skilled individuals working in or applying for cyber roles)
- The role of training and outsourcing to fill skills gaps
- Where the cyber security jobs market is active geographically
- The roles being labelled as cyber roles versus ones that are not but require a similar skillset
- The role that recruitment agents play in the cyber security labour market
- Diversity within the cyber sector
- Staff turnover in the cyber sector
- Candidate recruitment and staff retention strategies

For reference, any mention of 'cyber' throughout this report refers to the cyber sector. Any reference to 'cyber security' refers to how individuals and organisations reduce the risk of cyber attacks and is a component of working in a cyber sector role.

1.2 Summary of the methodology

This section contains a brief outline of the research methodology. Greater methodological detail can be found in the accompanying technological report.

The methodology consisted of 4 strands:

1. **Quantitative surveys** – Ipsos conducted representative telephone surveys with 4 audiences: general businesses, public sector organisations, charities, and cyber firms. These surveys gathered the main estimates on skills gaps and shortages reported in this study. Fieldwork was conducted between 14 July and 29 September 2022.

2. **Qualitative interviews –** Ipsos conducted a more focused strand of qualitative research, with 28 in-depth interviews split across cyber firms, other medium and large businesses, and recruitment agents. The interviews explored the challenges these organisations faced in addressing skills gaps and shortages, and the approaches they were taking on recruitment, training, staff retention, and workplace diversity. Interviews took place between August and October 2022.

[1] We refer to these studies by the publication year rather than the fieldwork year. Therefore, the report before this one is referred to as the 2023 study, even though the fieldwork was in 2022.

3. **Job vacancies analysis** – Perspective Economics analysed cyber security job postings on the Lightcast labour market database, showing the number, type and location of vacancies across the UK. This also covers remuneration, descriptions of job roles and the skills, qualifications and experience being sought by employers. This work covered vacancies across the 12 months of 2022 (i.e. January 2022 to December 2022), which provides a time series analysis building upon the previous 2022 study.

4. **Supply side analysis** – Perspective Economics replicated the methodology used on the 2021 cyber recruitment pool research to estimate the overall size of the current recruitment pool, as well as those likely to be entering the pool within the next 12 months (across 2023). This strand produces further statistics on the diversity, educational and occupational backgrounds, and salaries of this pool of labour, as well as outflows from the pool. In addition, this analysis explores graduate outcomes relating to cyber security employment across all disciplines.

1.3. Acknowledgements

Ipsos and Perspective Economics would like to thank Professor Steven Furnell from the University of Nottingham, the UK Cyber Security Council and the National Cyber Security Centre (NCSC) for their contributions to the qualitative topic guide.

We would also like to thank colleagues at DSIT for their project management, support and guidance throughout the study.

Who works in cyber security roles?

This chapter explores the people covering cyber security across organisations, including their career pathways into the role, their specialisms and the qualifications they hold.

For context, outside the cyber sector, we asked participating organisations to choose the staff member most responsible for their cyber security to complete the survey or interview. As in previous years' surveys, these individuals are typically not cyber professionals. The survey explores the extent to which such roles are formally labelled as cyber roles.

Key findings

- Half of businesses (50%) have just 1 employee responsible for cyber security. Larger organisations continue to be better resourced, although even in these organisations cyber teams of more than 5 people are very rare
- Within the cyber sector, 47% entered their current job after being employed in a previous cyber role. By contrast, outside the sector, staff performing cyber duties in-house are overwhelmingly transitioning from a non-cyber role (84%)
- When looking at the 16 specialisms aligned to the Career Route Map outlined by The UK Cyber Security Council, the highest prevalence across cyber firms was security generalists, with 61% of cyber sector firms having employees working in this role. Despite this high prevalence, results from the 2022 survey found that generalists comprised 26% of the cyber security workforce. Beyond these generalists, the distribution of cyber security roles in the sector is relatively evenly spread with between a fifth to two-fifths working in each

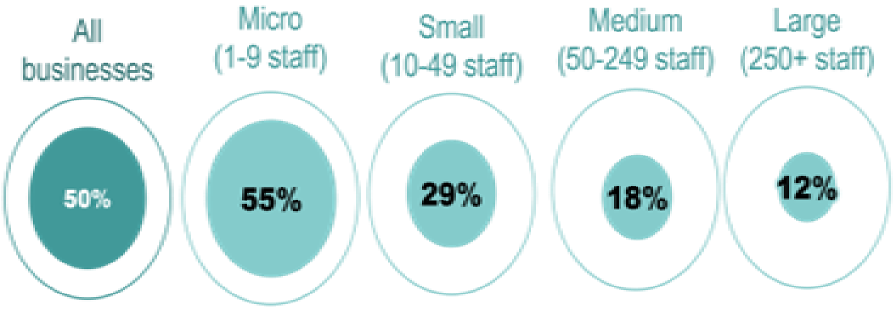
2.1. Size of cyber teams

Cyber teams outside the cyber sector

Across the private, charity and public sectors, cyber security responsibilities are typically assigned to either 1 person or a small handful of people. 50% of businesses and 47% of charities have just 1 employee who is directly responsible for managing or running their organisation's cyber security. Public sector organisations continue to be better resourced in this regard, with 17% having only 1 person in this role. The median team size for public sector organisations is between 2 to 3 people.

As Figure 2.1 illustrates, larger organisations tend to have bigger cyber security teams. Among both medium and large businesses, the typical (median) cyber security team comprises 2 to 3 people.18% of medium businesses and 12% of large businesses have 4 to 5 people in these roles.

Figure 2.1: Percentage of businesses with just 1 employee responsible for cyber security



Bases: 102 public sector organisations, 947 businesses; 442 micro; 248 small; 150 medium; 107 large

As was the case last year, these results are consistent across different sectors.

The businesses that outsource any aspects of cyber security tend to have better-resourced in-house cyber security teams than those who do not. 58% of those that outsource have more than 1 person responsible, compared to 43% of those who do not outsource. This could be due to larger businesses being more likely to outsource. While 33% of businesses outsource aspects of cyber security, this increases to 62% for large organisations.

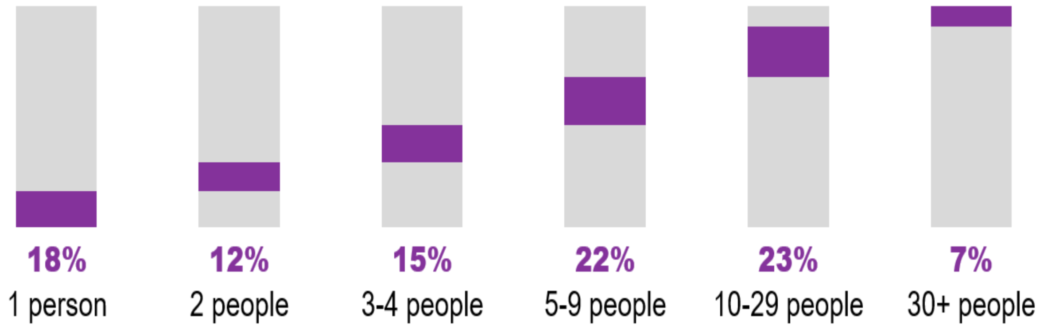
These findings are consistent with patterns in the previous years of the study. There has not been any significant expansion (or reduction) in the staffing of cyber security in organisations across the board.

Cyber teams within the cyber sector

Most firms in the UK cyber sector (i.e. those trading in cyber security products or services) continue to be smaller businesses. The DSIT [Cyber Security Sectoral Analysis 2023](#) finds that 62% of these firms are micro and 24% are small.

Our research finds that the typical (median) cyber team within cyber sector firms comprises between 5 and 9 people, i.e. at the higher end of the micro business bracket (Figure 2.2). These figures exclude people working in non-cyber roles in these businesses (e.g. admin roles, or other professional services or tech roles in diversified businesses). Our survey suggests team sizes have remained consistent with the previous year's study.

Figure 2.2: Percentage of cyber sector businesses employing cyber teams with the following number of people



Base: 174 cyber sector businesses

2.2 Career pathways into cyber roles

Career pathways into cyber roles outside the cyber sector

Among all the staff carrying out any cyber functions in the private sector, 84% have absorbed these tasks into an existing non-cyber related role (Figure 2.3). This is consistent with findings in the 2022 study. In these roles, cyber security may not be their only or top priority.

In the qualitative research, some participants had several roles and felt they could not devote sufficient time to their cyber security responsibilities. Examples of other responsibilities were operations, marketing, data protection as well as broader IT (e.g. infrastructure).

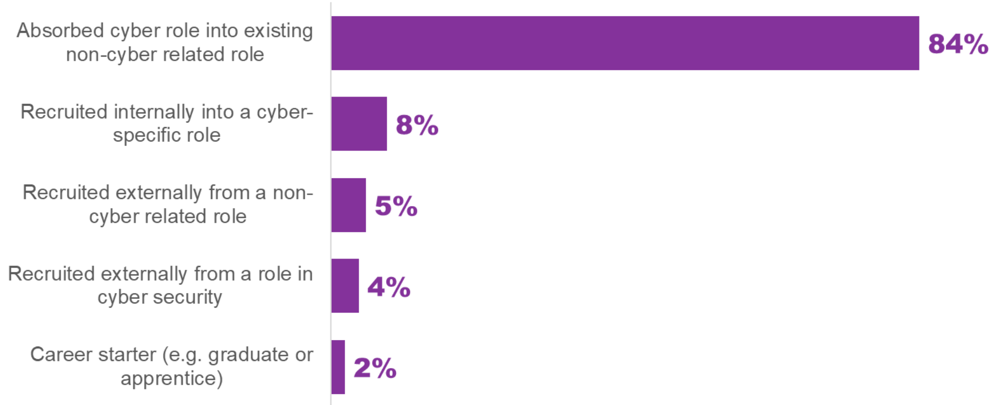
"It is one of many roles that fall under my remit. I don't give as much time to it as I would like to."
(Private sector organisation, 250-999 employees)

Participants reported feeling pressured and pulled in different directions. More broadly, some participants identified a lack of sustained resources for cyber security teams as their biggest challenge. Participants working in public sector organisations highlighted the impact of current spending constraints.

"At the moment, we're not getting funding streams through to do what we're doing…Budgetary constraints are incredibly ferocious at the moment. Cybersecurity is a 24/7 problem. And we're not paid to do that. So, everything's been done on kind of grace and favour and best endeavours outside of hours."
(Public sector organisation, 250-999 employees)

Where people are performing a dedicated cyber role, it is relatively rare for businesses to have recruited them from a previous cyber role in another organisation. However, this is higher in this year's study, rising from a negligible 1% to 4% in this year's study. As with the findings in the previous study, this suggests that most private sector firms continue to focus on transitioning staff who may not have cyber-specific technical skills (e.g. IT staff) into cyber roles, as a way of filling skills gaps.

Figure 2.3: Percentage of those in cyber roles outside the cyber sector who have come in through particular career pathways



Bases: c.1108 businesses (where answers given on team size and on how each individual came into the team)

In the qualitative research, private and public sector organisations did not generally have defined career pathways for cyber security roles. A lack of available roles was a key reason for this, but funding could also be an issue.

“There are currently no defined career pathways. The council won’t contribute to the costs. We currently are offering no career pathways in cyber roles and cannot offer any apprenticeships. You are expected to have the knowledge or experience already and, if a role becomes available, then to apply for this role.”
(Public sector organisation, 1,000 or more employees)

While there were no career pathways as such, some employers had trained staff up to take on cyber security roles. However, the cost of training was often a barrier, as well as taking time away from the job. As we go on to discuss in Chapter 7 on Staff Turnover, staff leaving for higher paid jobs following training could be an issue.

“There isn't much opportunity to undertake continued professional development. You are required to get on with the day-to-day job, as it is quite demanding."
(Public sector organisation , 1,000 or more employees)

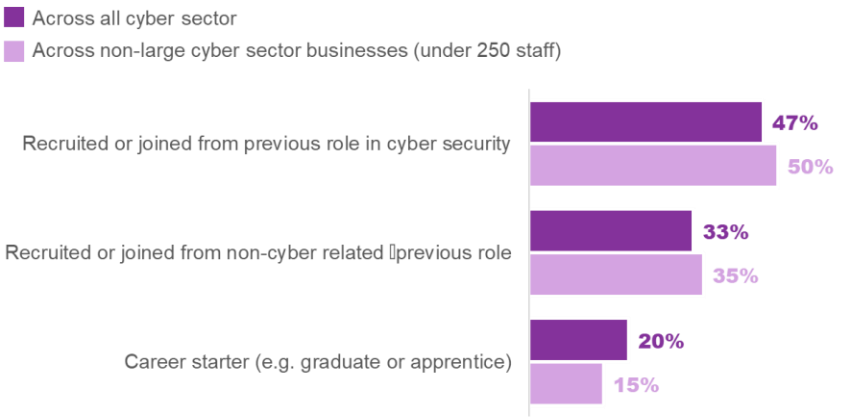
Career pathways within the cyber sector

Within the cyber sector, 47% of the cyber workforce entered their current role after working elsewhere in a cyber role, slightly down from 54% in 2022, while 33% came from the non-cyber sector, higher than the 2022 study (27%). These results are consistent with previous years of the study.

The other half have not come directly from a previous job in cyber security (but may have worked in cyber security earlier in their careers) – see Figure 2.4. The chart suggests that pathways into cyber roles tend to be more varied within the cyber sector than outside it.

Across the board, it is more common for employers to take on those already in the labour market rather than career starters (33% vs. 20%). However, the trend of more employers taking on career starters is maintained – in 2020, 12% of the cyber workforce in non-large cyber sector firms were new graduates or apprentices compared to 19% in 2022 and 20% now).

Figure 2.4: Percentage of cyber sector workforce who have come in through particular career pathways



Bases: 162 cyber sector businesses (excluding those that could not break down their workforce);

In the qualitative research, we found that large cyber firms had defined career paths starting from entry-level. These career pathways could be technical, consultancy or a hybrid, with flexibility to move between them. These firms had dedicated training budgets, but career progression was also supported through informal training and experience on the job.

"It is all focused around the individual and driving their own career. We try to train people through experience mostly. On each pathway, at each grade, we have standard external training qualifications and courses which are the starting point for people to achieve. We support them through our training budget in doing those."
(Cyber sector firm, 1,000 employees or more)

Smaller cyber firms did not have career pathways and career progression could be limited because the services provided were generalist or niche. Some did no formal training at all. As with private and public sector organisations, cost, time and losing staff were barriers to training.

"The training is there but it is costly. The certification programmes require quite a hefty cost for the training if you're going to send people off for the week. Because there is such a shortage of skills in the industry, a lot of organisations are reluctant to put employees through it because once they are qualified they are quite likely to move to another job on a higher salary."
(Cyber sector firm, 2-9 employees)

Are internships or work placements offered in the cyber sector?

29% of cyber firms reported offering any internships or work placements since the start of 2020 (approximately over an 18-month period). This is almost the same as last year (27%), and the previous year (28%) when this question was first asked. As was the case last year, this is higher for cyber security firms who are actively trying to recruit, with 47% of firms who have tried to recruit since the beginning of 2021 offering internships and placements in cyber security roles.

2.3. Specialisms of employees in UK cyber sector firms

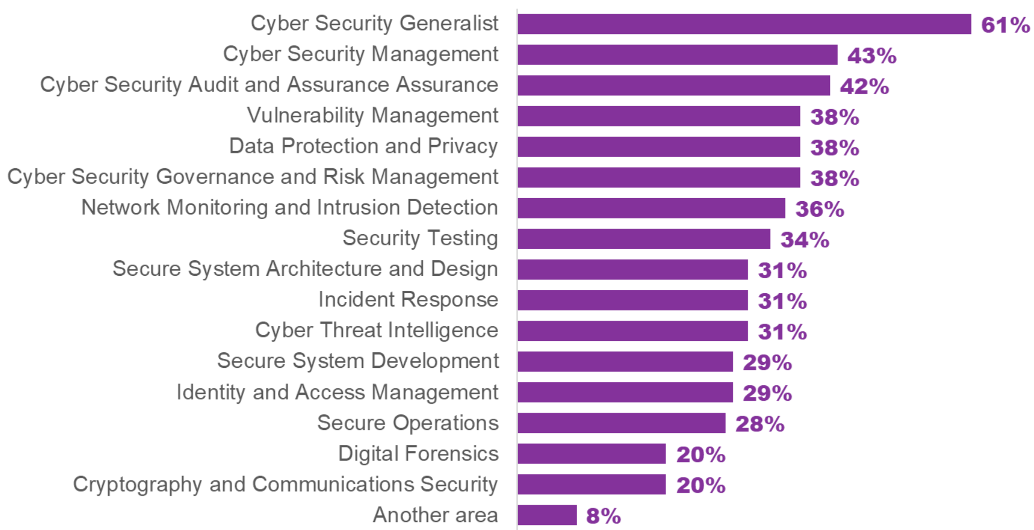
The UK Cyber Security Council is a self-regulatory body for the UK's cyber security profession. The Council has developed a Careers Route Map to make it easier for individuals to enter cyber security roles via a range of possible pathways. The Route Map is also intended to help employers and recruitment agents to understand the various pathways they can offer to jobseekers and existing employees.

Proportion of cyber sector workforce working in particular specialisms

This year, for the first time, the survey estimates the proportion of the cyber workforce within cyber sector firms that have employees working in each of the cyber security specialisms aligned to the Careers Route Map. The list of roles (shown in Figure 2.5) reflects the 16 cyber security specialisms included.

- These new statistics highlight the high prevalence of cyber security generalists, with 61% of cyber sector firms having employees working in this role. Despite this high prevalence, results from the 2022 survey found that generalists comprised 26% of the cyber security workforce. In the 2023 survey the definition outlined in the UK Cyber Security Career Route Map of a Cyber Security Generalist was “the performance of the duties of multiple cyber security specialisms in one role.” Respondents were also instructed to select Cyber Security Generalist if they felt the work they did was equally spread across the specialisms listed in the Careers Route Map
- Beyond these generalists, the distribution of cyber security roles in the sector is not skewed towards one specialism. After cyber security generalists,43% of cyber sector firms have employees in cyber security management and 42% in audit and assurance. Digital forensics and cryptography/communications security have the lowest proportion but there is a relatively even spread across the 16 specialisms.

Figure 2.5: Percentage of cyber sector workforce who have employees working in each of the 16 specialisms outlined in the UK Cyber Security Council's Careers Route Map



Bases: 137 cyber sector businesses where a specialism was specified

Qualitative feedback on the UK Cyber Security Council's Careers Route Map

Most employers and recruiters taking part in the qualitative research had not heard of the Careers Route Map or the 16 cyber security specialisms. A few of those who were aware of the Route Map had used it or had contemplated doing so. For instance, a recruiter was using it as training material to train other recruiters and help them understand the variety of skills and pathways.

"I use it to train some of my recruiters. I've been looking at this page for years now. It is the best thing out there beyond the shadow of a doubt."
(Recruitment agent)

A couple of large cyber firms had or were considering using the Route Map to standardise cyber roles.

"I have asked some of the people who work for me to have a look at that in terms of a standardisation approach rather than coming up with our own labels. Hopefully, that helps with recruitment and managing people and career pathways and things like that."
(Cyber sector firm, 1,000 or more employees)

Employers and recruiters generally felt it was useful to have individual roles and specialisms set out in the Route Map. This provided clarity about cyber security roles and could help with understanding what skills there were in their organisation and potential career progression for their cyber staff, as well as recruitment.

2.4. Qualifications of those in UK cyber sector firms

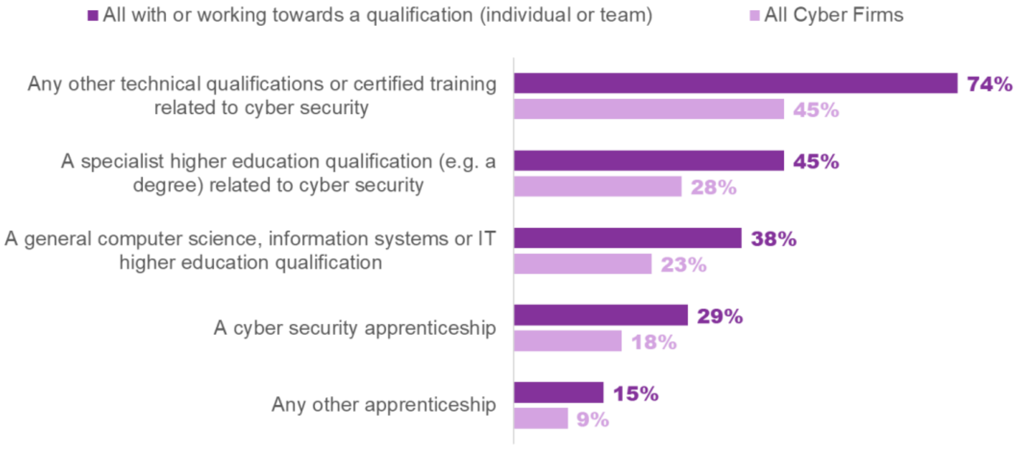
Prevalence of different types of cyber security qualifications

Given that cyber security is largely covered informally across the private (i.e. non-cyber) sector, our survey has historically focused on the qualifications of cyber staff in cyber sector firms.

In 2023, 61% of cyber firms say that they have any employees with, or working towards, a cyber security-related qualification or certified training. This is in line with 2022 (62%) but less than the 2021 study (70%). It indicates no clear trend upwards or downwards over the last 2 years.

Figure 2.6 highlights the kinds of qualifications or certifications that cyber firms say their staff have. Of note, these figures are based on all cyber firms, not just the 61% that say their staff have any relevant qualifications or accreditations. When combining the specific responses in the chart, 38% say they have any staff with a relevant higher education degree (in cyber security or computing), and 20%have any apprentices among their staff.

Figure 2.6: Percentage of cyber sector firms that have staff with the following types of qualifications or accreditations



Base: All Cyber Firms: 180, All with or working towards a qualification: 110

In the qualitative research, we found that large cyber sector firms aligned qualifications to career pathways, for instance, Certified Information Systems Security Professional (CISSP) in respect to general risk advisory work or the Council for Registered Ethical Security Testers (CREST) for security architects. For some cyber sector firms, ensuring staff hold certifications helped prove their credibility to their clients.

"Our credibility is based on providing credible consultants and the best way to demonstrate that is, not only their experience, but the certifications they hold."
(Cyber sector firm, 2-9 employees)

However, some small or micro cyber firms said they were unable to support staff in obtaining certifications.

Attitudes towards a potential Chartered status for cyber professionals

In October 2022, the UK Cyber Security Council announced a pilot programme to create the UK's first chartered cyber professionals. In the qualitative interviews, we explored views on having a Chartered status for individuals working in cyber security roles. Reactions were generally positive. Employers and recruiters in favour thought it would bring greater credibility to the profession and provide more confidence to employers in hiring.

"I'm a big fan of chartered status. Chartered cyber professional is great and would probably carry more weight than some of the certifications we are asking for at the moment."
(Cyber sector firm, 1,000 or more employees)

Another advantage of chartered status identified is motivating individuals by providing more structure to the profession.

"It shows you have a level of competence in your profession. As a motivator, it is good for people. It helps people feel they are progressing and achieving things."
(Private sector organisation, 250-999 employees)

However, a couple queried the relationship with certifications, such as CISSP, which were regarded as having a chartered status already.

Diversity in the cyber workforce

This chapter covers diversity in the cyber workforce, with an emphasis on gender, ethnicity, physical disability and neurodiversity[2]. This includes attitudes towards diversity from the qualitative research and estimates of the diversity of the cyber sector workforce from the quantitative survey.

Like in previous iterations, we focus on cyber sector firms in the survey questions on diversity, and not the wider business population, because cyber sector firms are the high-volume recruiters and employers of cyber roles. In addition, including wider businesses would provide a misleading picture of diversity in the cyber security labour market since the majority are performing cyber roles informally.

Key findings

- The proportion of the workforce that is female is 17% and 22% of the workforce is from ethnic minorities. This is not statistically significantly different from last year, when the figures were 22% and 25% respectively
- In line with previous years findings, the senior workforce (typically with 6 or more years of experience) tends to be slightly less diverse than those in more junior roles, in terms of gender, ethnicity, and disability status. For example, just 14 % of senior roles are filled by women
- Employers are still taking steps to increase the diversity of their workforce within the sector. 40% of cyber firms who have actively tried to recruit in the last 18 months have taken action to adapt their recruitment processes or have carried out specific activities to encourage applications from diverse groups

3.1. Estimates of diversity in the cyber sector

All-workforce statistics

The latest study shows that the proportion of the workforce that is female is 17%. This is slightly lower than the 2022 study (22%), but the difference is not statistically significant. In 2021 the figure was 16%. The proportion of the workforce from ethnic minority groups is 22% (vs. 25% in 2022). As with gender, the change from 2022 is not statistically significant.

It is important to highlight that since these are *workforce*-level estimates compiled from *employer* survey data – they estimate the percentage of the cyber workforce with certain traits, unlike most of the reported data which represents the percentage of employers – we do not expect to find statistically significant differences over time. Instead we focus on broad trends in the data.

A further consideration is that these estimates can be very variable and in calculating them in this and previous years we have removed any outliers. For example, in this study, for the female estimate, we have removed the largest business from the cyber sector sample as an outlier. If this outlier had been

[2] For this study (e.g. in question wording), we defined neurodiversity as the inclusion of people with conditions or learning disorders such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD).

included, the proportion of female workers would increase from 17% to 37%. However, this year's results are consistent with the 2021 findings (16%).

With these caveats in mind, the proportion of women in the cyber workforce has remained broadly consistent, standing at 15% in 2020, 16% in 2021, 22% in 2022 and 17% in 2023. Although there were signs of an upward trend last year, this has not been sustained.

The upward trend for ethnic minorities has been more consistent, rising from 16% in 2020 to 25% in 2022 but then plateaued this year on 22%. The upward trend for ethnic minorities has been more consistent, rising from 16% in 2020 to 25% in 2022 but then plateaued this year on 22%. Despite this plateau, figure 3.1 shows the Cyber sector remains ahead of the wider digital and UK workforce when it comes to employing those from ethnic minority backgrounds. 22% of the cyber sector workforce are from ethnic minority backgrounds compared to 18% of the Digital sector workforce and 14% of the UK workforce. This trend needs to be maintained in order to ensure diversity within the sector is improving.

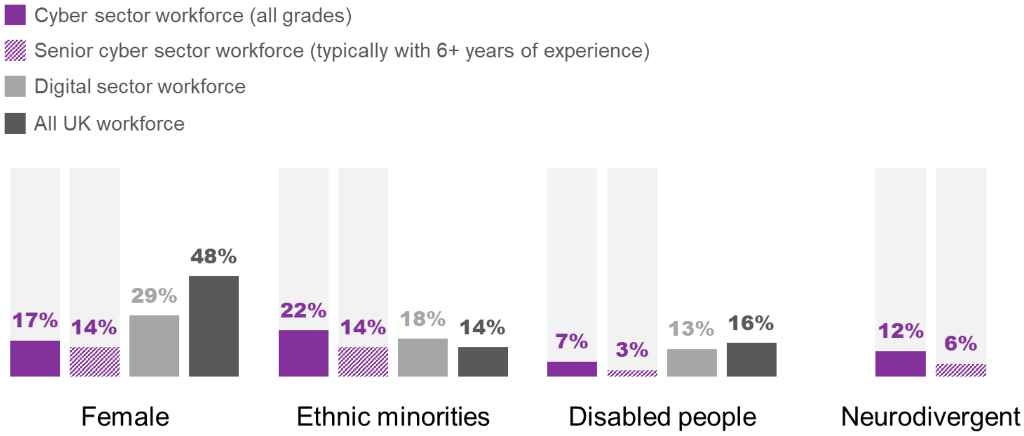
The full quantitative findings in Figure 3.1 show that sector diversity can be improved. The cyber sector remains behind other digital sectors with regards to gender diversity. For example, 29% of the UK digital sector workforce are female compared to 17% for the cyber sector workforce. The gap here also highlights that women with relevant transferable skills who could transition into cyber security are an untapped recruitment pool.

Our estimates are more in line with other digital sectors when it comes to diversity of ethnicities, with 18% of the UK digital sector workforce from ethnic minority backgrounds compared to 22% of the cyber sector workforce. For those with disabilities, the cyber sector workforce is slightly behind the wider UK digital workforce estimate. [^3] , with 13% having a disability compared to 7% of the cyber sector workforce. This overall pattern is unchanged from previous years.

A total of 12% of people in the cyber sector workforce are neurodivergent (i.e. people with conditions or learning disorders such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder, or ADHD). This is in line with previous years. There are no reliable statistics to show how neurodiversity overall compares to other sectors.

[3]Gender, ethnicity and physical disability comparison data comes from DCMS Sector Economic Estimates: Employment Apr 2021 – Mar 2022 - GOV.UK (www.gov.uk). We use the April 2021 to June 2022 data. .

Figure 3.1: Percentage of cyber sector workforce that come under the following diverse group



Bases: c.150-180 cyber sector businesses for all workforce estimates
(in each case excluding those that were not able to answer these questions, or refused)

Senior workforce statistics

Figure 3.1 also contains our estimates for the proportion of the senior cyber workforce that are from these diverse groups. We define senior cyber professionals as people who typically have 6 or more years of experience. The results suggest that there is slightly less diversity at this senior level than for the cyber workforce as a whole (within the cyber sector):

- 14% of all senior employees are from ethnic minority backgrounds (vs. 22% of the total cyber workforce)
- 14% of all senior employees are female (vs. 17%)
- 6% of all senior employees are neurodivergent (vs. 12%)
- 3% of all senior employees are disabled (vs. 7%)

Across all 4 groups there are no notable changes from last year or 2021. However, as we go on to discuss in the next section, some of the large cyber sector firms participating in the qualitative research felt that their senior leadership had become more diverse.

3.2. Attitudes towards workforce diversity

As has been the case in previous years, in the qualitative interviews, we found that diversity was predominantly seen in terms of gender and ethnicity. A couple also mentioned educational and socioeconomic backgrounds. Reflecting the quantitative findings, employers and recruiters regarded a lack of women as a particular issue for the sector. Neurodiversity was less on employers' radars but did come up, particularly in cyber sector firms.

Some cyber sector employers and recruiters thought that there had been some progress on diversity in the past few years with more women and/or ethnic minorities in the industry. This was attributed to a leadership and industry focus on improving diversity and a greater understanding of the benefits of a more diverse workforce.

"The industry, as a whole, is generally working on that with various initiatives to try and push diversity. I think people understood that the talent pool was wider, and that there were serious business benefits to diversity within security, whether that's through different experiences, different backgrounds, or neurodiverse candidates."
(Recruitment agent)

The large cyber firms taking part in the qualitative research highlighted that their senior leadership had become more diverse and that there was more diversity at entry level as well. The biggest issue was in the middle ranks – where the skills shortage is most acute.

"It has got a long way to go. But I am extremely proud of this, half of our partners are women. Where I struggle is that middle ground, mid-range up to the senior people. There is a good ethnic mix but not a good female/male split."
(Cyber sector firm, 1,000 or more employees)

While acknowledging the commitment to increase diversity in the sector, some employers highlighted that there was still a lot to do. One cyber sector firm emphasised the importance of different parties working together.

"There is a strong desire to put it right. It's a multi-party solution. You can't singlehandedly put it right. The sector needs a collaborative approach involving all stakeholders. Companies. Government. Education. Everybody."
(Cyber sector firm,10-49 employees)

3.3. Diversity and retention

None of the employers or recruiters we spoke to in the qualitative research had seen any particular patterns in terms of diversity and retention. Attrition was not noticeably greater in diverse groups. However, one recruiter highlighted that female, ethnic minorities and staff living with disabilities could face challenges in the workplace that other employees do not due to poor treatment and a lack of appropriate support systems.

Some employers had organisation-wide initiatives to support people in diverse groups and to make their senior leadership more diverse. An employer from a large cyber sector firm highlighted the use of promotions and bonuses to retain people from low socioeconomic backgrounds. For organisations with small cyber teams of one or two staff members, these wider initiatives may have limited impact.

"Once people are in the company there is a whole range of different communities of diversity and inclusion interests. 70% of our workforce is signed up to one community or another."
(Cyber sector firm, 1000 or more employees)

3.4. Diversity in recruitment processes

53% of cyber firms have tried to recruit people into cyber roles since January 2021 (our survey focused on activity over approximately the last 18 months before the interview).

Among this group, 40% have taken any action to adapt their recruitment processes or carried out specific activities to encourage applications from diverse groups. By action we refer to any cyber organisations who have tried to recruit people in the last 18 months who have made changes in order to recruit more women, people from ethnic minority backgrounds, neurodiverse/learning disorders or physically disabled people). In total, 18% of cyber firms have taken action across all four of these groups.

Firms are slightly more likely to have targeted women than other groups:

- 38% say they have made changes to recruit more women
- 31% made changes for people from ethnic minority backgrounds
- 26% did so for people with neurodiverse conditions or learning disorders
- 22% did so for physically disabled people

These figures are similar to what we found last year.

3.5. What are employers and recruitment agents doing to improve diversity?

In the qualitative research, employers taking steps to improve diversity in recruitment were often focusing their efforts on entry level positions. Examples included:

- Setting diversity metrics in graduate recruitment. A challenge identified here is that male/female ratios on cyber security degrees are still not 50/50. As we discuss in Chapter 10, the gender gap for cyber security courses remains wide, with only 12 % of female graduates at undergraduate level, and 23% at postgraduate level
- Hiring through non-degree routes using ‘capture the flag’ tests.[4][^3] to identify raw talent
- Working with third sector organisations to help identify and support more diverse groups
- Hiring neurodiverse people through the Kickstarter scheme. Two of the people hired had been long-term unemployed
- Working with the National Crime Agency to help find work for people from a mix of backgrounds who have a chequered past

The large cyber sector businesses that we interviewed were supporting a number of initiatives such as TechSheCan, as well as talks and competitions at schools to encourage women and ethnic minorities into the sector. These firms were also supporting networking and career programmes for diverse groups, notably women, who were already working in the sector.

“It is about trying to get more diverse talent at a school level and trying to get them to realise that there is a path which isn’t just for males.”
(Cyber sector firm,1,000 or more employees)

[4] ‘Capture the flag’ tests are gamified exercises designed to test cyber security skills.

At non-entry level, efforts focused on avoiding any bias in the recruitment process, most notably writing neutral and clear job descriptions or dropping the requirement for a degree for candidates with an appropriate level of experience. Some employers said they worked with recruitment agencies to find more diverse candidates. However, the recruiters that we interviewed reported that this can be challenging.

“My response is: Ok. It's 2022. There's no 50-50 shortlist. Let's be serious about this."
(Recruitment agent)

A couple of the recruiters we spoke to explained how they worked with their clients to help them tackle barriers to inclusion and success in the sector. For example, carefully wording job descriptions to reduce the likelihood of people self-rejecting or being unnecessarily excluded (for instance degree requirements) and ensuring that interviews are held in accessible spaces.

"I can't change the marketplace but I can encourage clients to have conversations about it….It's about asking questions every step of the way and making your client realise their privilege - therefore what adaptations can be made."
(Recruitment agent)

However, many of the employers taking part in the qualitative research reported difficulties recruiting staff from diverse groups. As we have found in previous years, the key barrier here is the candidate pool. Some employers recounted receiving applications from mostly males, with one private sector organisation saying that in the last three years they had only had one female applicant out of hundreds of CVs. Other employers found recruiting candidates from ethnic minorities a challenge because their local area is not diverse.

"It’s not very diverse as we don’t have the talent pool and the area that we are in is not very diverse within itself.”
(Public sector organisation, 1,000 or more employees)

Another issue was that some employers did not have a diverse recruitment strategy. They said they wanted to give the job to the best candidate, regardless of background. There was also a sense of uncertainty about how to recruit more diverse groups. One public sector organisation which had found that 90% of candidates were men said:

"That disparity is huge. So, for all we would like to recruit more diversity we're not seeing it come in. There's a bit of a question there: are we doing the right things to recruit the right people? But to a certain extent, we can only respond to the market that we've got."
(Public sector organisation, 250-999 employees)

Cost was another barrier identified by a cyber sector business, one cyber sector firm which had made plans to invest in diverse recruitment but had put this on hold because the new contracts which it was about to win had fallen through.

Greater diversity will widen the talent pool. There is a need for interventions to encourage diverse groups into cyber careers. Initiatives such as the UK Cyber Security Council's previously mentioned Careers Route Map also have an important part to play in supporting individuals with transferable skills to transition into cyber roles. This is particularly the case for employers who do not have the resources to recruit cyber staff at entry level.

Current skills and skills gaps

This chapter explores the cyber security skills that organisations feel they need and the size of current skills gaps. Cyber security skills gaps exist when individuals working in or applying for cyber roles lack particular skills necessary for those roles. This is different from skills shortages, which are when there is a shortfall in the number of skilled individuals working in or applying for cyber roles – we cover skills shortages with regards to recruitment in Chapter 5.

Key findings

- Half (50%) of all private sector businesses identify a basic technical cyber security skills gap, i.e. a lack of confidence in performing a range of basic cyber security skills tasks or functions. This estimate is in line with previous years. It accounts for around 739,000 UK businesses
- A third of businesses (33%) have a more advanced technical skills gap, in areas such as penetration testing, forensic analysis, security architecture or engineering, threat intelligence, interpreting malicious code and user monitoring. This is also in line with previous years. It accounts for around 487,700 businesses
- Half of all cyber firms (49%) have faced problems with technical cyber security skills gaps in the past 12 months, either among existing staff (22%) or among job applicants (44%).
- Just over 4 in 10 cyber sector firms (43%) have experienced a complementary skills (or soft skills) gap in this timeframe. This is consistent with last year (when it was 41%)

4.1. Technical skills gaps outside the cyber sector

As has been the case in the 4 previous labour market studies, we asked organisations to report how confident they would be to carry out specific cyber security tasks or functions that require various skills. Those who say they are not confident are understood to have a skills gap in this area.

Where organisations outsource a cyber security task or function to external service providers, we do not count this as a skills gap. We cover the proportions outsourcing each task in Chapter 9.

Basic technical skills gaps

The survey explores organisations' ability to confidently cover a range of basic technical cyber security tasks and functions. They are a combination of the technical areas covered under the government-endorsed Cyber Essentials scheme[5] and other basic aspects of cyber security highlighted by DCMS. As shown below in Table 4.1, confidence in carrying out these tasks has remained consistent across all 4 years of this study.

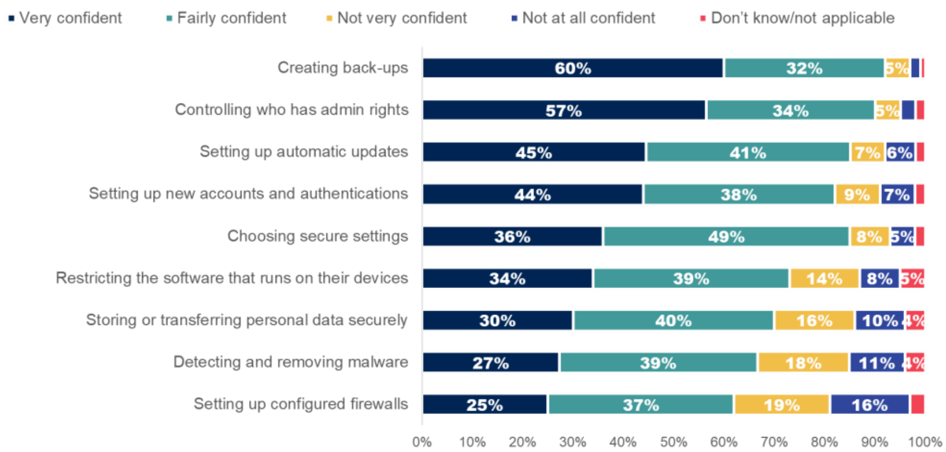
[5] Cyber Essentials is a government-endorsed accreditation scheme for organisations to demonstrate that they meet a minimum cyber security standard. As part of this, organisations need to implement basic technical controls in 5 areas (boundary firewalls and internet gateways, secure configurations, user access controls, malware protection and patch management).

Table 4.1: Extent to which businesses are very confident or fairly confident carrying out each of these basic skills gaps across all 4 years of the study (Base is where such tasks are not outsourced except for setting up new accounts and authentications)

Basic technical skill	2023	2022	2021	2020
Creating back ups	92%	93%	93%	89%
Controlling who has admin rights	91%	86%	88%	85%
Setting up automatic updates	86%	87%	88%	82%
Choosing secure settings	85%	80%	85%	82%
Restricting the software that runs on their devices	73%	74%	78%	78%
Storing or transferring personal data securely	70%	71%	67%	68%
Detecting and removing malware	66%	66%	72%	68%
Setting up configured firewalls	62%	62%	62%	62%

As Figure 4.1 shows, the areas where skill gaps are most prevalent are, setting up configured firewalls, detecting and removing malware, storing or transferring personal data securely, and restricting software that runs on business-owned devices. These were the most common areas in all previous years too (excluding dealing with cyber security breaches or attacks, which is incorporated as part of incident response). As we have seen in previous years, only a minority of cyber security leads across the business population say they are not confident in carrying out each of these tasks. Setting up new accounts and authentications were not asked about in previous waves of the survey, so therefore cannot be trended.

Figure 4.1: Extent to which businesses are confident in performing basic cyber security tasks (Base is where such tasks are not outsourced except for setting up new accounts and authentications)

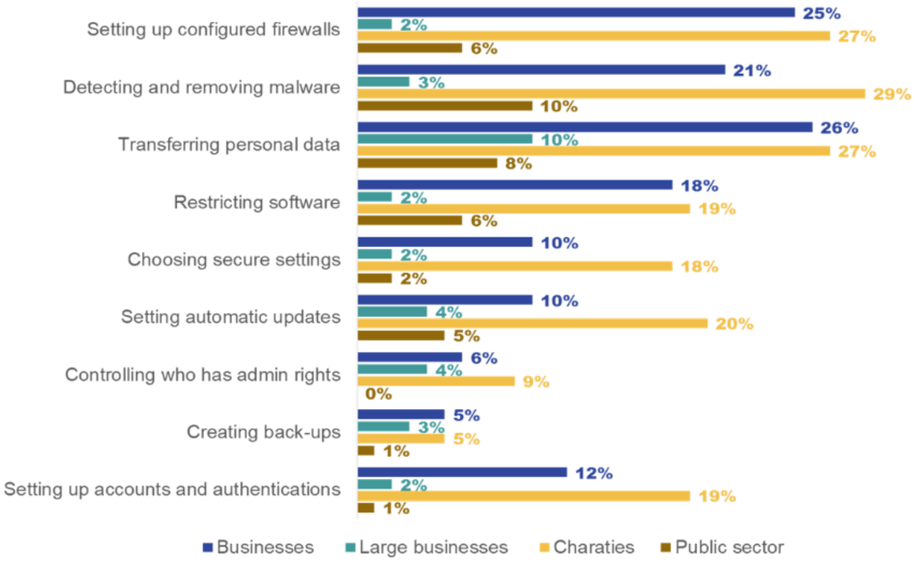


Bases: c.765+ businesses that do not outsource each task
Unlabelled bars are under 4%.

Figure 4.1 does not include businesses that outsource these tasks or functions, as by outsourcing they do not need the skills to perform these tasks in-house.

Figure 4.2 therefore rebases the proportion that are not confident out of all businesses (i.e. including the businesses that outsource cyber security in the base) to give a fuller picture of the proportion with a particular skills gap in the total population. It also shows skills shortages by type of organisation. Across all these areas, large businesses and public sector organisations are less likely to report skills gaps. In previous years, charities have been more likely than businesses to have skills gaps across the board. While the charted results here indicate the same pattern, the differences between businesses and charities (encompassing all size bands) this year are not statistically significant.

Figure 4.2: Percentage not confident in performing basic cyber security tasks, by type of organisation



Bases: 1006 businesses; 78 large businesses (with 250+ staff); 214 charities; 102 public sector organisations
N.B. these figures are rebased on the full survey samples, but the questions are only asked of a subsample. The subsamples are very small for large businesses, charities and public sector organisations (c.78+).

These figures across all organisations are not significantly different from last year's study, highlighting the ongoing need for basic cyber security advice and guidance to organisations outside the cyber sector.

Information and communications businesses continue to be among the least likely to identify basic skills gaps across this list of tasks. There are also indications, in line with previous years, that some of these basic technical skills gaps are more prevalent in the food and hospitality sector and construction sector, as well as the entertainment, service or membership organisation sector.

A combined basic technical skills gap indicator

For a general sense of the number of organisations that have a basic skills gap, we combine all 10 tasks listed in Figures 4.1 and 4.2, to calculate the overall percentage of organisations that are not confident in carrying out at least 1 of these basic tasks. From this, we calculate that 50% of businesses have a basic technical cyber security skills gap. Reflecting the pattern seen in previous years, this estimate is higher for charities (57%), and lower for public sector organisations (19%) and large businesses (18%).

This is a representative survey based on the UK business population, allowing us to make inferences on the total number of businesses with basic skills gaps. Extrapolating the overall business figure of 50% to the overall population of private sector businesses, we estimate that approximately 739,000 businesses in the UK have a basic technical skills gap.[6]

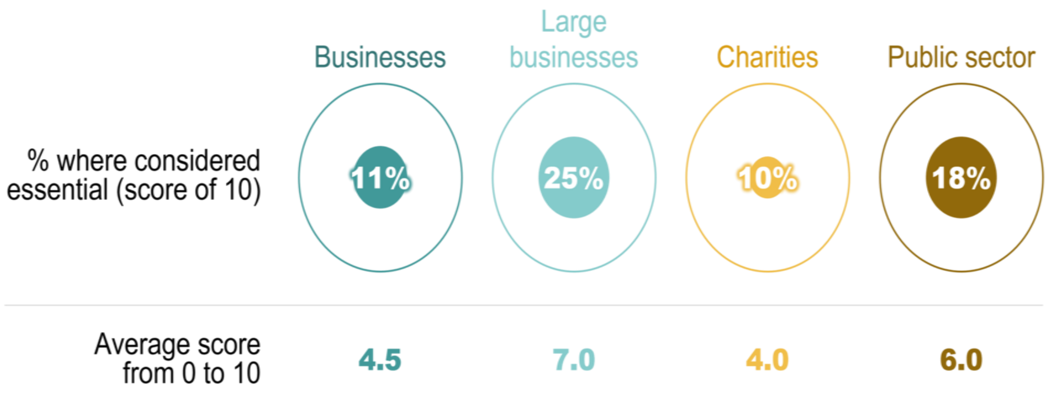
Perceived importance of advanced technical skills

All organisations require basic cyber security skills that enable them to implement basic cyber hygiene measures. Beyond this, some organisations may, based on their perceived level of risk, judge that more advanced technical skills are required.

Our definition of advanced technical skills was developed through extensive scoping research carried out as part of the [2018 cyber security labour market study](). It includes any skills associated with security architecture or engineering, penetration testing, using threat intelligence tools, forensic analysis, interpreting malicious code or using tools to monitor user activity. These are skills that we expect may not be required in every organisation but will be important for those with more sophisticated cyber security needs.

We asked organisations to rate how important it is for their in-house cyber security teams to have these sorts of skills. A score of 0 means it is considered not at all important, while 10 means it is essential for cyber security teams to have these skills. Figure 4.3 shows that these kinds of technical skills are more in demand in large businesses and public sector organisations than in other types of organisation. These findings are in line with previous years.

Figure 4.3: Perceived importance of advanced cyber security skills for those working in cyber security roles outside the cyber sector



Bases: 1,006 businesses; 78 large businesses (with 250+ staff); 214 charities; 102 public sector organisations

These advanced technical skills are considered to be more important among the information and communications sector (24% vs. 12% overall), which is also consistent with previous years.

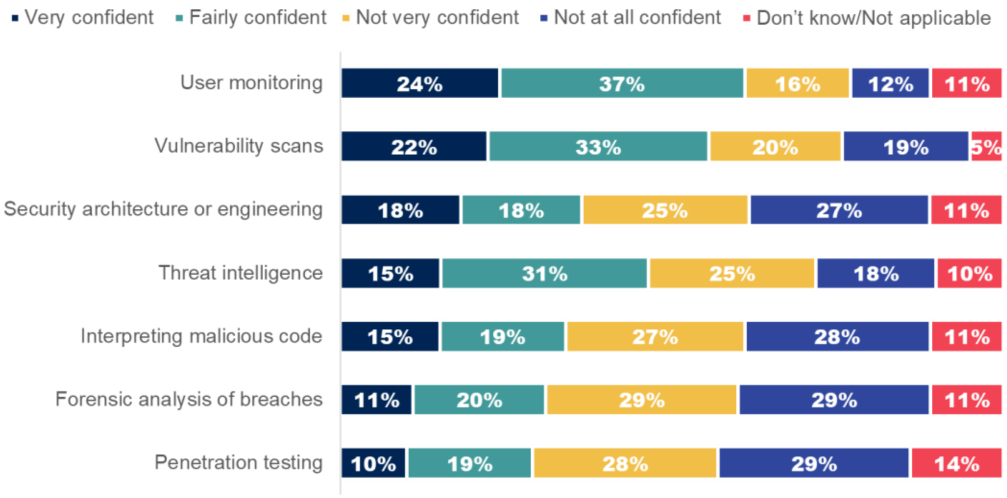
---

[6] The business population data is taken from the BEIS Business population estimates in 2021, which estimates 1,365,805 private sector businesses with employees, outside the agricultural sector (which is excluded from this research). This is the latest estimate as of the publication of this report. For the extrapolated figures presented here and later in this chapter, we have rounded to 3 significant figures. These figures are of course subject to a margin of error, as with all the results from the survey. The margin of error for businesses on this result is ±4.3 percentage points. This means that the true figure could be between approximately 638,000 and 755,000 businesses. We have not made the same kind of extrapolation for charities or public sector organisations, given the relatively small sample sizes for these 2 groups.

Advanced technical skills gaps

Figure 4.4 illustrates businesses' advanced skills gaps in the cases where businesses consider this suite of skills to be important for their organisation[7] and do not outsource these areas of cyber security. In other words, where businesses have self-identified that they need these types of skills in-house. It suggests that gaps in advanced cyber security skills are most prevalent when it comes to forensic analysis of breaches, security architecture, interpreting malicious code and penetration testing. The results are consistent with last year's findings, with no significant differences found between the 2022 and 2023 study.

Figure 4.4: Extent to which businesses are confident in performing advanced cyber security tasks (where such tasks are identified as important for the business and not outsourced)



Bases: c.464+ businesses that do not outsource each task

In Figure 4.5, we rebase these findings to show all businesses (therefore including those that either outsource these tasks or do not consider them to be important). This again gives a fuller picture of the proportion of the total population that has advanced skills gaps. It also compares this to charities and public sector organisations. There are too few large businesses sampled at this question to be reported here.

In interpreting this data, it is important to note the following assumptions:

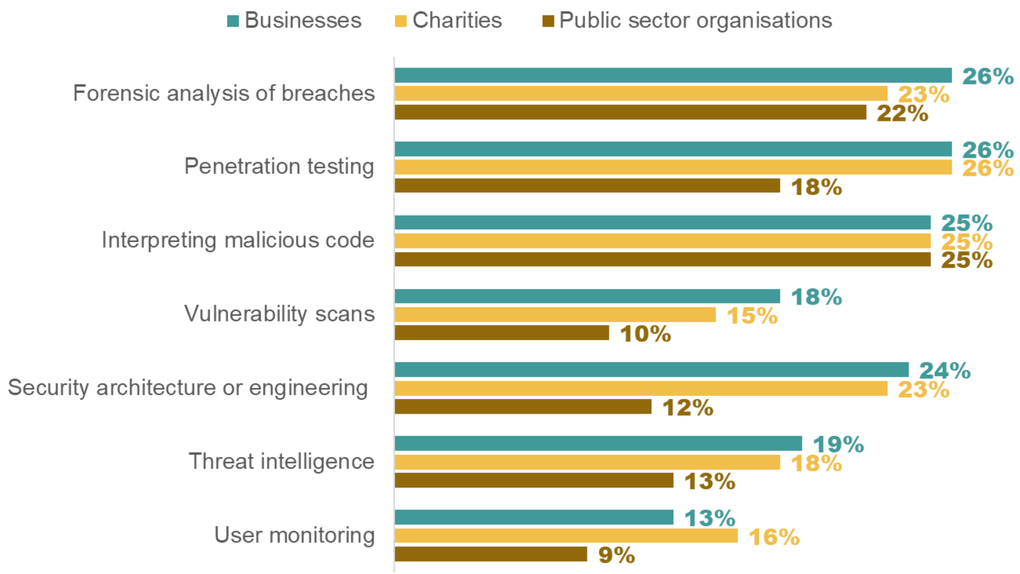
- We assume that the organisations outsourcing these areas of cyber security to an external provider do not have skills gaps (i.e. the external provider fills any gaps)
- We also assume that if organisations do not consider these advanced areas to be important for them, then they do not have a skills gap (recognising that, for example, not all organisations require penetration testing to manage their cyber risks)
- These are self-identified skills gaps, where the cyber security lead in an organisation admits to not being confident in carrying out technical tasks in these areas

Figure 4.5 shows that the top advanced skills gaps – in interpreting malicious code and forensic analysis – tend to be similarly prevalent across different types of organisations. Across some of the advanced

[7] This is defined as organisations giving a score of 5 or more (out of 10) when asked about the importance of having access to advanced technical skills (Figure 4.3).

skills, a lower proportion of public sector organisations report not being confident performing them. These functions include carrying out vulnerability scans and penetration testing. These findings are broadly in line with previous years. The exception is confidence in interpreting malicious code which is directionally lower compared to the 2022 study (25% for businesses vs. 17% last year).

Figure 4.5: Percentage not confident in performing advanced cyber security tasks, by type of organisation (Base out of all organisations)



Extrapolating advanced technical skills gaps across the business population

Continuing to use the rebased proportions from Figure 4.5, we can approximate the number of private sector firms that have skills gaps in each of these more advanced technical areas of cyber security:

- Around 369,500 (25%) have a skills gap in forensic analysis (vs. 26% last year)
- Around 354,700 (24%) have a skills gap in interpreting malicious code (vs. 17% last year)
- Around 339,900 (23%) have a skills gap in penetration testing (vs. 24% last year)
- Around 325,100 (22%) have a skills gap in security architecture (vs. 24% last year)
- Around 266,000 (18%) have a skills gap in threat intelligence (vs. 18% last year)
- Around 266,000 (18%) have a skills gap in vulnerability scans (no 2022 data available)

A combined advanced technical skills gap indicator

Following the same process as the basic cyber security skills gap calculation, we have merged the 7 advanced cyber security tasks referenced in Figures 4.4 and 4.5, to calculate the percentage of organisations that are not confident in carrying out at least 1 of these tasks.

33% of businesses have an advanced technical skills gap which equates to approximately 487,700 of UK businesses. 32% of charities and 30% of public sector organisations also have an advanced skills gap. These results are consistent with last year's study.

4.2. Technical skills gaps within the cyber sector

Overall prevalence of technical skills gaps

The quantitative data in this section comes from a survey of the cyber sector carried out as part of the DCMS Cyber Security Sectoral Analysis 2023. The survey methodologies used in both the sectoral analysis and this cyber security skills study are the same.

22% of cyber sector employers report having existing employees who lack necessary technical skills. Just 3 % of employers specifically say this prevents them meeting their business goals to a *great* extent, while 20 % say it does so to *some* extent.

By contrast, around double this number of cyber firms (44%) say that the job applicants they have seen lack necessary technical skills. In total, 19% say this has affected their ability to meet their business goals to a great extent, and 25% to some extent.

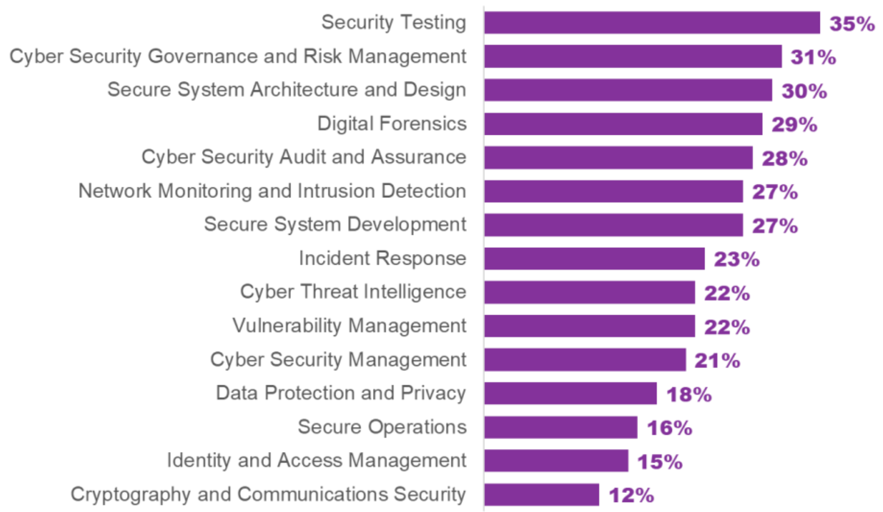
Both these figures remain lower than in the 2020 survey, and more in line with last year's results. The technical skills gap measure is 10 percentage points lower for existing employees than in 2020 (when it was 32%) and 14 percentage points lower for job applicants than in 2020 (when it was 59%). In each year, the question was framed consistently, looking back at skills gaps over the previous 12 months.

Areas in which there are technical skills gaps

Combining these results indicates that 49% of cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants. Again, this combined score is lower than the 2020 result (when it was 64%) and is consistent with last year's result (49% in 2022). The increase in technical skills gaps in 2020 could be due to factors relating to the COVID-19 pandemic. As more trend data is collected in subsequent years, we will have a clearer picture of whether this was a temporary rise.

Among this 49% that have had any issues with skills gaps, Figure 4.6 illustrates which specific skillsets are considered lacking. The categories are based on the Chartered Institute of Information Security (CIISec) Skills Framework.

Figure 4.6: Percentage of cyber firms that have skills gaps in the following technical areas, among those that have identified any skills gaps



Base: 220 cyber sector businesses identifying any skills gaps

In summary, there is still an overall shortfall of a wide range of specific skillsets.

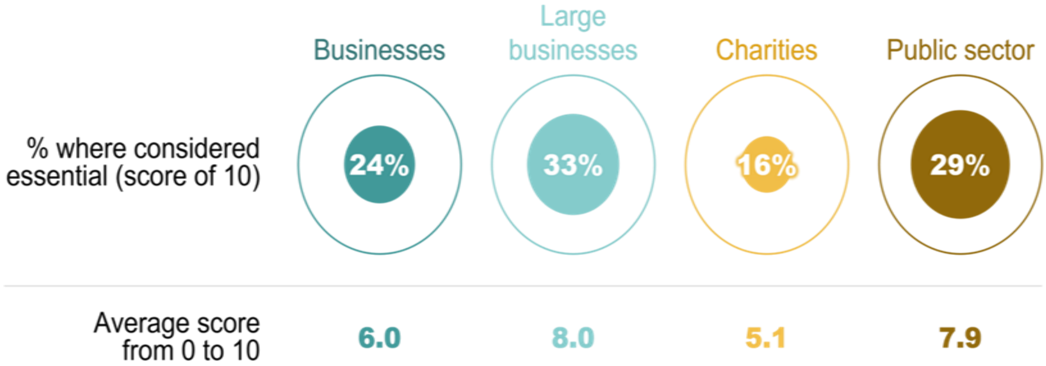
Due to the way in which this question was asked in the sectoral analysis survey in 2023, the results are not able to be directly comparable to the 2022 results.

4.3. Incident response skills

Perceived importance of incident response skills outside the cyber sector

Many organisations do not recognise the importance of in-house incident response skills. We again asked organisations to rate how important it is to have these skills, where a score of 0 means not at all important, and 10 means it is essential. Figure 4.7 shows that 24% of businesses consider these skills to be essential, rising to 33% of large businesses, around 29% of the public sector and 16% of charities (16%).

Figure 4.7: Perceived importance of incident response skills for those working in cyber security roles outside the cyber sector



Bases: 1,006 businesses; 78 large businesses (with 250+ staff); 214 charities; 102 public sector organisations

The incident response skills gap

Incident response remains a challenging area for organisations. It is one of the top areas covered by external providers – of the 33 % of businesses that outsource any aspect of cyber security, 82% utilised an external cyber security provider to deal with incident response and recovery. We found in the qualitative research that even if incident response is outsourced, it may still be a concern for organisations.

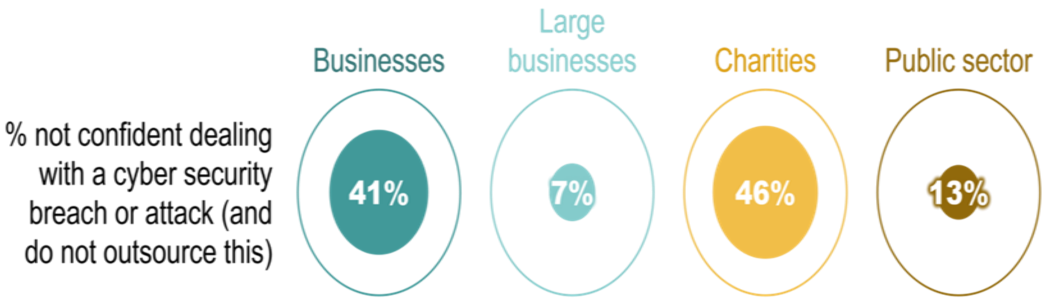
"If we think about the organisation including the managed service provider, the biggest skills shortage is around the understanding of how to deal with incidents."
(Public sector organisation, 1,000+ employees)

Among those organisations that do not outsource this function, 41% are not very or not at all confident that they would be able to deal with a cyber security breach or attack. This totals to 41% of all UK businesses when rebased to include those who outsource incident response – shown in Figure 4.8.

Although not statistically significant, the percentage of businesses not confident in carrying out activities related to incident response has risen again this year. If we look at the data since 2020, we can see that it is trending upwards (from 27% in 2020, to 32% in 2021 and 37% in 2022).

There were no statistically significant differences by sector found on this measure.

Figure 4.8: Percentage not confident in carrying out activities related to incident response



Bases: 736 businesses; 39 large businesses (with 250+ staff); 184 charities; 65 public sector organisations
N.B. these figures are rebased on the full survey samples, but the question is only asked of a subsample. The subsamples are very small for large businesses and public sector organisations (c.60+).

The qualitative research highlighted the challenge of finding the right resources to deal with cyber security breaches and attacks.

“There is a low level of understanding of what to do with incident response. I've even found with qualified IT security people, because they don’t have to do incident response very often, sometimes when they need to do a basic one, they need help."
(Public sector organisation, 1,000+ employees)

46% of businesses are also not confident in their ability to write an incident response plan. This is consistent with the previous years (49% in 2022 and 45% in 2021). Similar to businesses, 40% of charities say they are not confident. This is lower than last year’s study (55% in 2022) but consistent with 2021 findings (44%). The proportions who are not confident in public sector organisations (19%) is similar to last year (23%).

4.4. Complementary skills

The perceived importance of complementary or soft skills in the cyber sector

The survey results show that cyber sector businesses are, by and large, aware of the importance of complementary skills (sometimes referred to as soft skills). We asked these firms to rate how important it is for those in cyber roles to have complementary skills, where a score of 0 means not at all important, and 10 means it is essential. The average result, similar to the 2020, 2021 and 2022 scores, is 8.4 out of 10. (32%) give the top answer of 10.

Do cyber sector firms identify a complementary skills gap?

The following quantitative results come, once again, from the cyber sector survey carried out as part of the DSIT Cyber Security Sectoral Analysis 2023 (which used a comparable methodology). They are reported here for the first time.

32% (the same figure as last year), say that, over the last 12 months, they have seen job applicants for cyber roles lacking communication, leadership, management, or sales and marketing skills. A total of 3%

say this has stopped them meeting their business goals to a great extent while 22% say this is to some extent.

24% say that their existing employees lack these complementary skills, with 3% saying this impacts them to a great extent and 21% to some extent. This figure has been relatively stable across the 3 years of available cyber sector data.

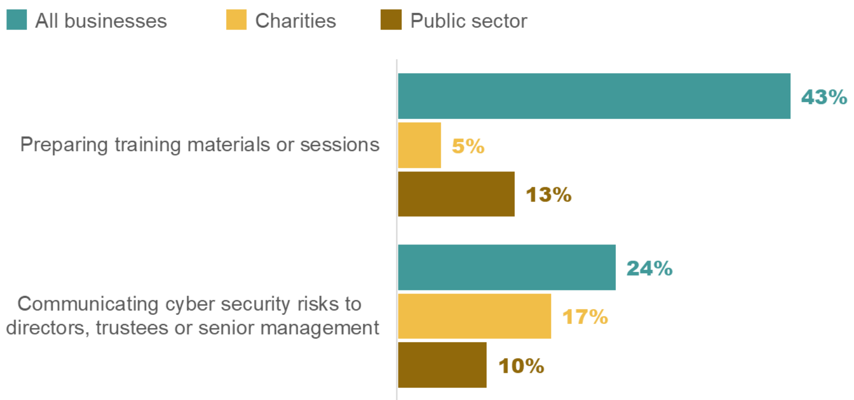
When combining these scores for existing staff and job applicants lacking complementary skills, we find that 43% of cyber sector employers have experienced a complementary skills gap in the previous 12 months. This is consistent with last year (41%).

As was the case in the previous year, this is not far off the proportion of firms experiencing technical skills gaps (49%), suggesting that a lack of complementary skills remains a big issue for cyber sector.

Ability of cyber leads outside the cyber sector to undertake tasks requiring complementary skills

With organisations outside the cyber sector, the survey covers confidence in cyber leads being able to carry out specific activities such as developing training, communicating risks and communicating good practice. These tasks require a mix of technical knowledge and complementary skills in order to be done successfully. Figure 4.9 illustrates the proportion of organisations that reported skills gaps in these areas. As in previous years, only a minority of organisations feel confident in training staff or communicating cyber security risks to their senior leadership.

Figure 4.9: Percentage not confident in carrying out a range of tasks that require a mix of technical and complimentary skills



Bases (asked to a random half of full sample): c.486 businesses; c.88 charities; c.58 public sector organisations.

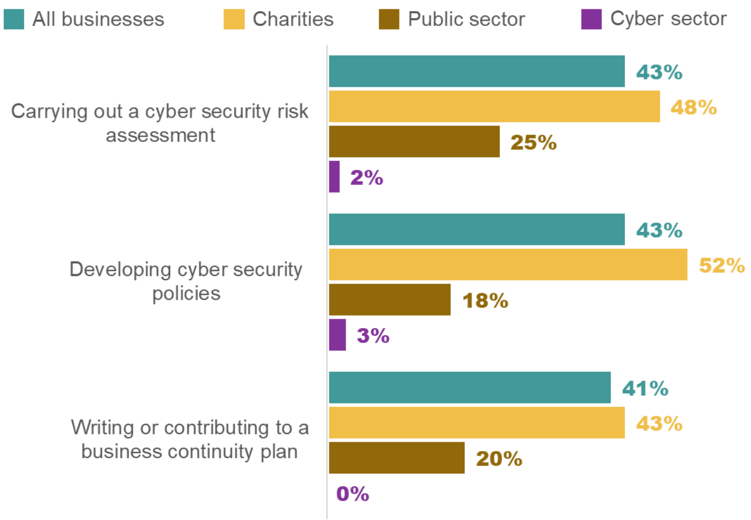
4.5. Governance and compliance skills

When it comes to people in cyber security roles being able to carry out cyber security governance tasks, there are widespread self-identified skills gaps. As Figure 4.10 suggests, 43% of private sector cyber security leads are not confident in their ability to carry out a cyber security risk assessment or develop cyber security policies. 41% of businesses also lack confidence in writing the cyber security aspects of business continuity plans.

We also ask these questions of cyber sector businesses, which continue to be overwhelmingly confident at being able to carry out these tasks for their own organisations, with less than 5% saying they are not confident in each area.

These findings are, again, in line with the previous labour market surveys.

Figure 4.10: Percentage not confident in carrying out a range of cyber security governance tasks



Bases (asked to a random half of full sample): c.511 businesses; c.101 charities; c.44 public sector organisations; c.92 cyber sector businesses

Elsewhere in the survey, we establish the perceived importance of this broader governance, risk and compliance knowledge among cyber sector employers. 42% say it is essential for their staff to have an understanding of the legal or compliance issues affecting cyber security. This is in line with the 2022 results (when it was 41%) and continues to indicate a widespread demand for staff to have this sort of knowledge.

4.6. Cyber security skills gaps in the non-cyber workforce

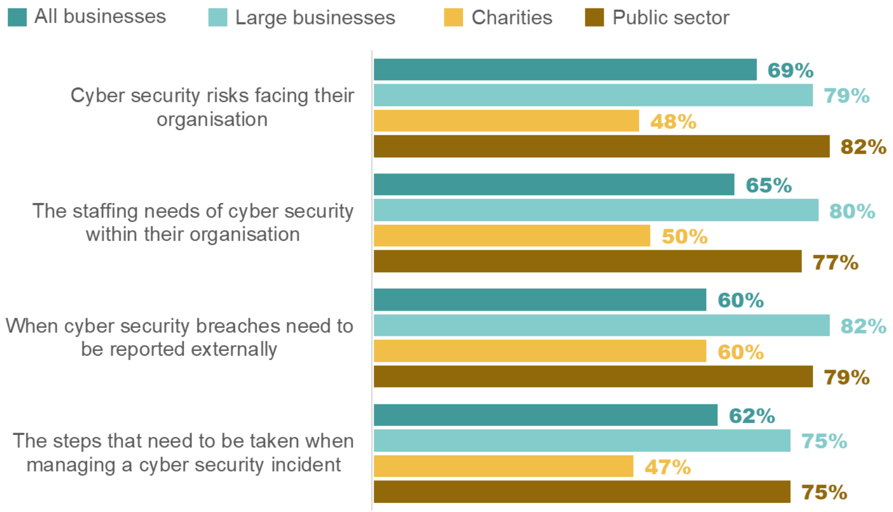
Senior managers and wider staff outside of cyber security teams also need to have the right skills and knowledge to be able to understand and interpret cyber security risks, recognise their governance and risk responsibilities, and follow the cyber security rules and processes set by their organisation. This section explores skills and knowledge gaps among these groups

Cyber security skills at the board level

Figure 4.11 shows the proportion of cyber security leads outside the cyber sector who think their management boards understand cyber security requirements. In the private sector, 40%do not think that their senior managers understand when cyber security breaches need to be reported externally and the steps that need to be taken to manage a breach. 35% report that their senior managers do not understand the staffing needs of cyber security within their organisation or the cyber security risks facing the organisation. The indicators on incident response, staffing, cyber security risks organisations face, reporting of cyber breaches externally tend to be less positive in charities.

These figures have not trended upwards or downwards consistently across the 4 years of this study and remain in line with last year's results.

Figure 4.11: Percentage of cyber team leads that feel their organisation's senior managers understand the following aspects of cyber security very or fairly well



Bases: 1,006 businesses; 78 large businesses (with 250+ staff); 214 charities; 102 public sector organisations

Across these indicators, cyber security leads in the finance and insurance sector and information and communications sector have a more favourable opinion of their senior management, whereas those in the construction sector tend to be less favourable than average. For example, 88% in finance and insurance firms and the same percentage (88%) of information and communications firms say their senior management understand the cyber security risks facing their organisation. This compares to 61%of those in the construction businesses.

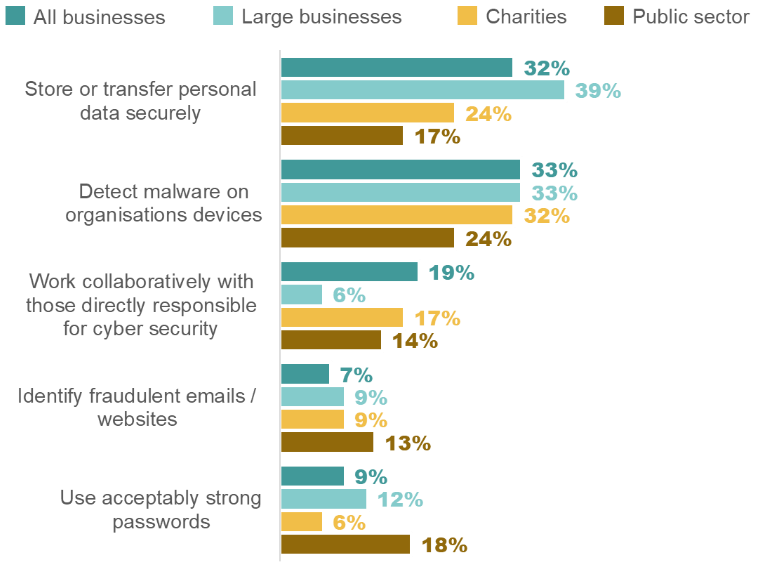
Cyber security skills among wider staff

When looking at the wider staff across all businesses (i.e. not in-house cyber teams or board-level staff), cyber security leads are, by and large, confident that they can carry out various tasks without negatively impacting the organisation's cyber security.

Figure 4.12 shows the list of tasks we cover in the survey, and the proportion that are <u>not</u> confident. It shows that the greatest concerns that cyber security leads have are around staff not being able to store and transfer personal data securely and not detecting malware on their devices. Moreover, in the public sector, there is more scepticism about staff using acceptably strong passwords than in businesses (18% not confident, vs. 9% across all businesses).

These results are consistent with previous years' findings – although the percentage that say they are confident in their wider staff's ability to deal appropriately with personal data remains higher than the 2018 baseline (67% confident now, vs. 58% in 2018).

Figure 4.12: Percentage not confident in non-specialist staff being able to carry out various tasks that can impact on cyber security



Bases: 1,006 businesses; 78 large businesses (with 250+ staff); 214 charities; 102 public sector organisations

Across several of these indicators, cyber security leads in information/communications and finance/insurance businesses again tend to be more confident than average about their wider staff acting appropriately when it comes to cyber security. For instance, on personal data handling, cyber security leads in the information/communication sector (86%) and the finance/insurance sector (71%) were more likely to rate their staff highly (compared to 65% average across the public and private sectors). This was also the case for cyber security leads in the health and social care sector (79%, a mix of public and private).

Qualitative findings on cyber security skills among board level and wider staff

In the qualitative research, some cyber security leads said a lack of awareness among staff in their organisation about cyber security risks was a key challenge. Examples were ensuring that staff were regularly changing passwords or would recognise potential phishing attempts. One participant from a public sector organisation said that despite providing cyber security training annually and to new joiners, each week they had to deal with someone clicking on a dangerous link. A couple attributed this lack of understanding to staff not having experience of cyber attacks.

"The biggest [challenge] would be, as an organisation, getting everybody on board. First and foremost, if you haven't been personally affected, then it's not as serious to you. Just realising how vulnerable you can be will wake you up to the point where you realise what information you're actually putting on your phones or your devices. We have to embed it into the culture."
(Public sector organisation, 50-249 employees)

As we have heard in previous years, it can be a struggle to engage senior leadership with cyber security at all.

“I don’t know what we can do to get [the workforce] on board. Even the board have no interest at all in cyber security. They see it as an inconvenience, something that needs to be done. They will baulk at the cost.”
(Private sector organisation, 50-249 employees)

In some organisations, senior leadership acknowledged the importance of cyber security but did not necessarily prioritise it as much as cyber security leads would have liked. For this public sector organisation, a close call with a cyber incident prompted a greater focus on investment in cyber security.

"We had a near miss with a cyber incident. It was near enough to basically be a real wake up call for the organisation to go: this is on our doorstep. That has really kick started a conversation of not just investing in staff, but investing in the kind of technology to help us deliver the job as well."
(Public sector organisation, 250-999 employees)

Recruitment and skills shortages

This chapter deals with organisations' approaches to recruitment, skills shortages – a shortfall in the number of skilled individuals working in or applying for cyber roles – and the challenges and barriers organisations face when trying to address skills shortages.

The quantitative survey findings on this topic are exclusively for cyber sector businesses, given that they are the high-volume recruiters in the cyber security labour market. We focus on job vacancies since the start of 2021.

The qualitative data is broader, as it covers the 3 groups that we interviewed: cyber sector businesses, medium and large organisations outside the cyber sector, and recruitment agents who recruited cyber security roles.

We also undertook a secondary data analysis of cyber security job vacancies, which covers many of the recruitment issues raised in this chapter from a different perspective. These findings are covered separately in Chapter 6.

Key findings

- More than half of cyber sector businesses (53%) have tried to recruit someone in a cyber role since the beginning of 2021. The average number of vacancies per firm has gone up from 6.8 in the 2022 report to 8.2 this year
- The most common recruitment approaches continue to be using recruitment agents (42% of the firms with vacancies), social networks such as LinkedIn (39%) and word-of-mouth recommendations (39%)
- Just under 4 in 10 cyber vacancies (37%) posted since the start of 2021 are reported as being hard to fill, which is slightly lower than the estimate from last year (44%) and in line with the year before (37%). The most common reason given for this continues to be around candidates lacking technical skills or knowledge
- Skills shortages are in generalist roles (where candidates are expected to understand a range of cyber security areas, but not necessarily in depth) and specialist roles in equal measure

5.1. Approaches to recruitment

53% of all cyber sector businesses have tried to recruit someone in a cyber role since the beginning of 2021. This is the same as the previous year's result. It is worth noting that the average (mean) number of vacancies per firm continues to increase and has gone up year on year from 5.2 in 2021 to 6.8 in 2022 to 8.24 this year.

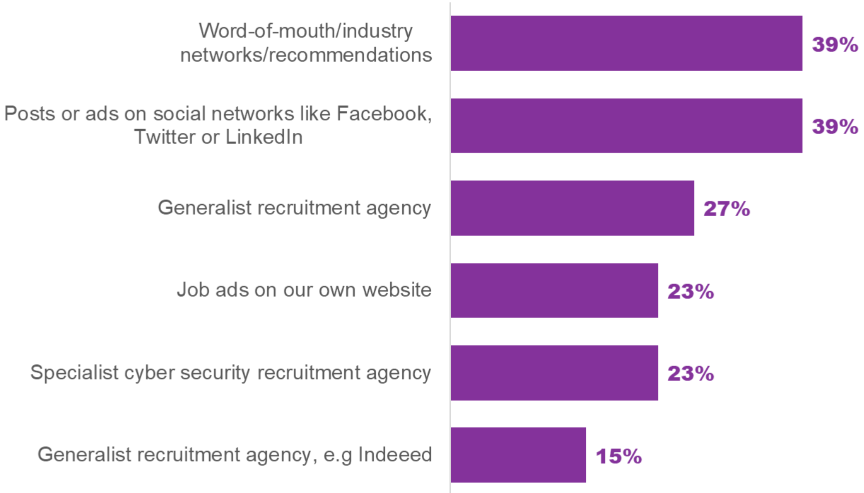
The rest of the survey findings in this chapter focus on the 53% of the sector who have tried to recruit someone (and later, on those that have specifically had hard-to-fill vacancies).

Most common recruitment methods

Figure 5.1 shows the recruitment methods used by the 53% of businesses that have had vacancies for cyber roles. Social networks, word-of-mouth recommendations and recruitment agents (either generalists or specialists) continue to be the most common approaches.

The findings are consistent with what we have found with the previous year's study, although word-of-mouth has moved up to first equal with social networks (both on 39%). 27% of cyber firms use generalist recruitment agents ,while 23% use specialists which, when combined, equates to 50% of cyber sector employers with vacancies.

Figure 5.1: Percentage of cyber firms with vacancies that have used the following recruitment methods (unprompted – multiple answers allowed



Base: 62 cyber sector businesses that have had vacancies in cyber roles since the start of 2021
Only specific categories mentioned by 10% or more shown.

As in previous years, firms undertaking recruitment in the sector tend to stick to a small set of tried-and-tested recruitment approaches. 35% of the cyber firms that have had vacancies have used just 1 of the methods mentioned in Figure 5.1 to fill these vacancies. In contrast 21% of cyber firms have used 2 methods and 26% have used 3 or more methods.

Entry-level recruitment

In the qualitative research, some employers felt that recruiting staff at entry-level was one solution to skills' shortages. For instance, one public sector organisation had taken the decision to develop talent internally because of the challenges they had experienced in recruiting senior people.

"We can probably grow our own to a certain extent, I think there is limits to that but obviously, that's fine, but it pays off in five years' time. Not right now. It's an investment not a solution." (Public sector organisation, 250-999 employees)

Some employers felt that there were many willing candidates keen to join the cyber security sector.

However, there were several barriers to offering entry-level roles. Some employers were reluctant to take on staff without any experience, even candidates with relevant educational qualifications like a cyber security degree.

"It's not a particularly easy field to get into. You could do a degree in cyber security but you're going to come out of that and people will say: 'that's fine but what networks have you worked on? What have you actually done?' The price of entry is high."
(Public sector organisation, 250-999 employees)

Time and money were important factors raised. Some employers said they did not have the resources for training apprentices or other entry-level staff. This could explain why in the quantitative research, recruiting internally (9%) and at junior levels (the use of graduate schemes is 9%) were less popular than other methods.

"We don't offer entry-level roles but there is discussion amongst senior management to offer apprenticeships in future positions in the near future. There is just no funding to enable us to offer these positions at the moment."
(Public sector organisation, 250-999 employees)

Another issue highlighted is that retaining junior staff can be problematic due to challenges in providing suitable salaries once they were more experienced and a lack of career pathways (see more in Chapter 7 on Staff Turnover).

As a recruiter pointed out, an unwillingness to recruit entry-level staff limits the growth of the talent pool.

"The biggest issue is that the industry itself runs on candidates' experience and people having a certain experience….because it is such a sensitive area for a lot of enterprises, they want someone who's been there and done that, first and foremost. So, it perpetuates the fact that there is a limited talent pool. And that limited talent pool is what everyone is fishing from, instead of driving new talent into it."
(Recruitment agent)

Qualitative findings on recruitment methods

The recruiters interviewed in the qualitative research (all of whom specialised in cyber recruitment), indicated that the bulk of their recruitment of candidates in the cyber sector were through referrals from networks. These were networks they had spent significant amounts of time and energy developing over the years, for instance through building their own profile.

"The most impactful way that I have found sourcing candidates is building our brand specifically as a cyber professional. I will post a lot about what's going on in the marketplace."
(Recruitment agent)

Recruiters used LinkedIn for sharing word-of-mouth recommendations and building a network, as well as job postings. In contrast recruiters considered other job boards the least effective way of recruiting candidates, in particular for hard-to-fill vacancies.

Word-of-mouth recruitment was also favoured by employers, some of whom offered referral bonuses to staff. These personal networks could act as something of a vetting process. Recruiting senior staff sometimes enabled employers to tap into their individual networks so they could ‘bring’ staff with them.

“We get a fair number of people who have worked together previously and that is a really good route. We know they’ve got the right kind of culture and so on.”
(Cyber sector firm, 1,000 or more employees)

Employers were adopting a range of strategies to tackle the challenges in recruiting cyber staff and attracting them to come to work for them. Similar approaches were being used for staff retention (for more detail see Chapter 7 on Staff Turnover). Employers offered candidates opportunities for development, interesting work and a positive work culture.

“We persuade people on the basis of opportunity. We’re growing fast, we’ve got a good track record but we’ve still got further to go. There is tons of room to move up. We use technology heavily in the business so there is the opportunity to expand and experience those tools.”
(Private sector organisation, 250-999 employees)

Some employers offered candidates tailored benefits packages, pension contributions and hybrid or remote working, as well as funding for training.

However, recruiters and employers regarded salary as key to successful recruitment. Employers did generally benchmark salaries against industry norms (some used IT rather than cyber benchmarks) and were aware that they needed to offer salaries which were the market rate. But both employers and recruiters felt that the competitiveness of the job market was pushing up salary requirements, particularly for hard-to-fill roles.

“Because of the hotness of the market, some people’s salaries went up by 25%.”
_(Cyber sector firm, 1,000 or more employees)

As we have found in previous years, some employers struggled to meet the going rate on salaries.

"They're going to market rates, which is difficult if you do any research into what the going rate for a cyber specialist with the CISSP qualification is, it's quite a big number. And that doesn't align particularly wonderfully with local government pay scales."
(Public sector organisation, 250-999 employees)

Another strategy adopted by employers was casting the geographical net wider to access more talent.

"We started going more national. We used a specialist IT recruitment company in London. We upped the salary quite considerably, and that then resulted in successful recruitment."
(Public sector organisation, 250-999 employees)

This has been facilitated by the widespread prevalence of remote and hybrid working as a result of the COVID-19 pandemic. For some employers, this had proved to be very beneficial.

"A lot of our clients saw great successes when they opened up to remote working and hybrid working. Thinking about utilities business in the Midlands, they really struggled with their location to find cyber talent. They went remote for the pandemic and decided to rethink their remote working strategy. They could attract talent nationwide."
(Recruitment agent)

As well as enabling employers to access more talent, hybrid or remote working can make an employer a more attractive proposition to candidates.

However, some employers preferred staff to work in the office for various reasons such as team-building, line management, learning from others, and security set-up.

“Since Covid, there has been a lot of expectation around working at home permanently as opposed to working back in an office again. We need the person to be here at least a few days a week. We are trying to get candidates open to that.”
(Cyber sector firm, 2-9 employees)

A few employers found it even harder than before to recruit as local candidates were being siphoned off to work for organisations further afield which could offer higher salaries.

“Traditionally, we would compete with other local organisations. Now, we're competing with London based salaries."
(Cyber sector firm, 10-49 employees)

For some organisations, the advantages of offering remote working were not sufficient to overcome their inability to compete with other employers on salary.

>"We do offer remote working opportunities but this from my perspective hasn’t improved the recruitment challenges we encounter, as the main problem is that we can’t offer high salaries compared to similar roles in other cities."
_(Public sector organisation, 1,000 or more employees)

Qualitative findings on job specifications

We found in previous years that a key challenge in recruitment was unrealistic requirements in job specifications. Recruiters shared similar feedback this year. High demands around skillsets, experience and qualifications could deter potentially suitable candidates.

"Some of the demands are unrealistic because they don't have an indication of what the market looks like. One of the things that has been most challenging is to explain to them the change

when it comes to remuneration, salary, expectations."
(Recruitment agent)

Recruiters explained how they acted as a liaison between their clients and candidates, taking on a role of translator or ‘guide’ of the job specification. They educated clients on labour market challenges and helped them craft effective job specifications which identified the essence of what was required.

"There's a difference between what they say and what they need. My question always is: Why do you need this?"
(Recruitment agent)

Recruiters regarded drafting the job specification, and the process of recruitment more generally, as a collaborative process between them and their clients. Successful recruitment required skilful negotiation and mediation as well as ability to foster trust with both clients and candidates. Recruiters said that clients seemed to be more flexible and open to listening to them because of current challenges in the labour market.

5.2. Hard-to-fill vacancies

Among the 53% of cyber sector firms that have had any cyber security vacancies since the start of 2021, 67% had at least one vacancy that they considered to be hard to fill. This is the same as the result recorded in the previous 2022 study.

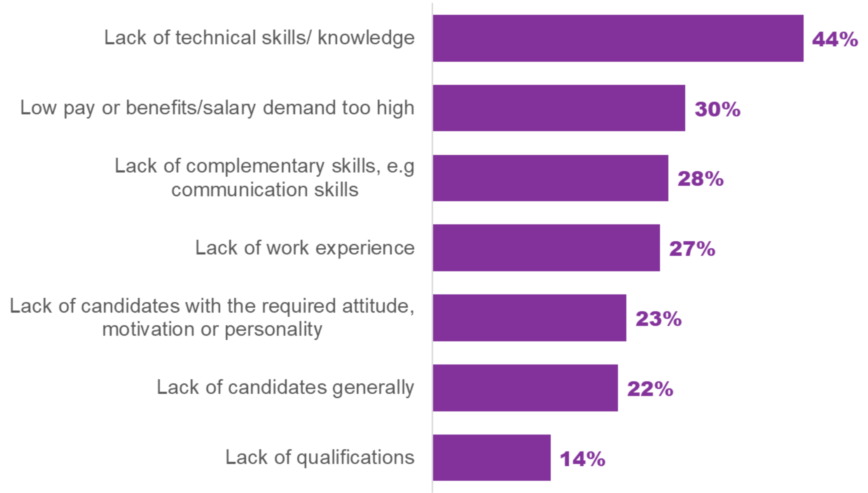
From another perspective, we estimate that 37% of all the *vacancies* posted since the start of 2021 are hard-to-fill vacancies, which is slightly lower than the estimate from last year (44%) and in line with the year before (37%). This is indicative evidence that the cyber security skills shortage has remained relatively consistent despite increasing demand for candidates to fill cyber roles (which we cover in Chapter 6). More years of data would be required to properly validate this trend.

Reasons behind hard-to-fill vacancies

As Figure 5.2 shows, among the 67% of cyber sector firms that have had hard-to-fill vacancies, the single most common reason given for this (without prompting) remains applicants lacking technical skills and knowledge. This was also true in the 2022 and 2021 studies.

The percentage of cyber firms reporting low pay or benefits/salary demand is 30%, while a similar proportion mention candidates with a lack of complementary skills (28%). 23% cite a lack of the required attitude, motivation or personality. Cyber businesses citing a lack of work experience as a reason for having hard to fill vacancies is 27%.

Figure 5.2: Most common reasons offered by cyber sector businesses for having hard-to-fill vacancies (unprompted – multiple answers allowed)



Base: 64 cyber sector businesses that have had hard-to-fill vacancies in cyber roles since the start of 2021
Only specific categories mentioned by 10% or more shown.

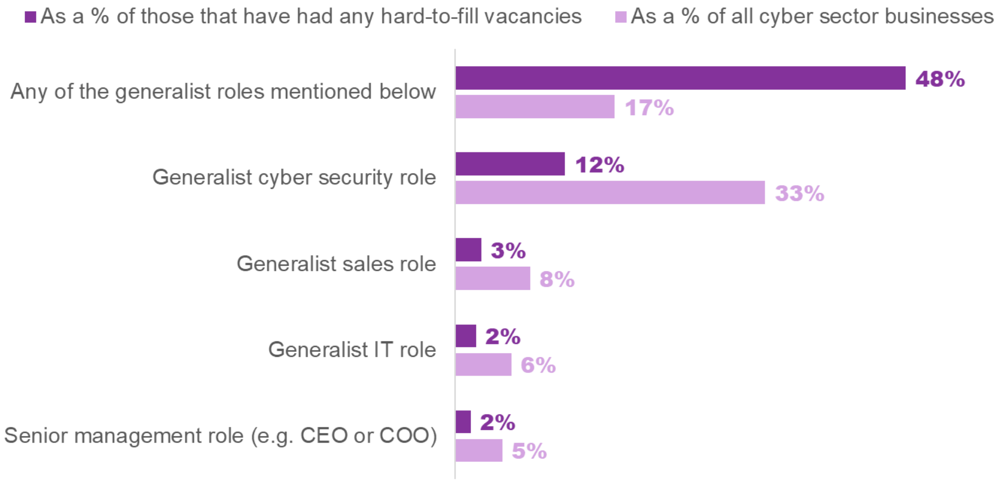
Specific roles most affected by skills shortages

The survey findings suggest that there are skills shortages across both generalist and specialist cyber roles in approximately equal measure. Among the cyber sector businesses that have had hard-to-fill vacancies, 48% say they have had such vacancies in generalist roles (Figure 5.3). This amounts to around 17% across the overall sector population. These results are in line with last year.[^8]

In this context, generalists are people who might be expected to understand and discuss a wide range of cyber security areas, but not necessarily in depth. It includes positions that primarily cover cyber security functions but without a particular specialism, senior management roles in cyber sector firms (e.g. on the executive board) as well as IT and sales roles that require cyber security knowledge or involve cyber security functions.

[8] In the 2022 report, we treated senior management roles as specialist roles, whereas this year, we have regrouped them into the set of generalist roles, in line with the new DCMS categorisation. Given the regrouping, these results are in line with last year.

Figure 5.3: Percentage of cyber sector firms that have found it hard to fill the following generalist job roles (multiple answers allowed)

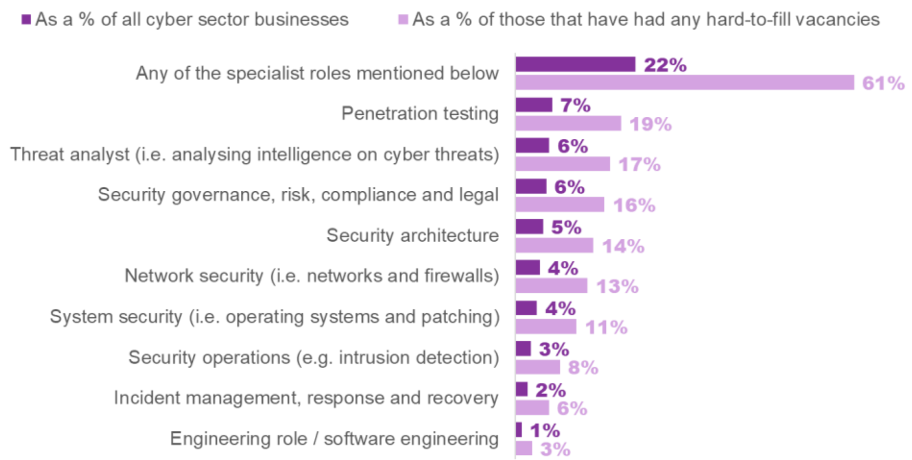


Bases: 180 cyber sector businesses; 64 that have had hard-to-fill vacancies in cyber roles since the start of 2021

Among those that have had hard-to-fill vacancies, 61% have had such vacancies in specialist roles. This equates to 22% of all cyber sector firms. Figure 5.4 shows how this breaks down, highlighting that the most common skills shortage is for penetration testers. By contrast, skills shortages in network security, system security and incident management are, relatively speaking, less common.

Consistent with the 2022 study, penetration testing tops this list by a very small margin. However, it is one of the least common job roles being advertised across the labour market (see Chapter 6). Therefore, this continues to be a niche skillset that is hard to come by, for the relatively small number of firms that require it.

Figure 5.4: Percentage of cyber sector firms that have found it hard to fill the following specialist job roles (multiple answers allowed)



Bases:180 cyber sector businesses; 64 that have had hard-to fill vacancies in cyber roles since the start of 2021

Qualitative evidence on hard-to-fill roles

In the qualitative research, some recruiters and cyber sector firms said that all cyber roles were currently hard to fill.

"The cyber security market is extremely dynamic, companies are fighting over talent. Requirements are often complex, hard to fill. There is a relatively small pool of candidates for any given role."
(Recruitment agent)

Some employers and recruiters had found that roles requiring advanced technical skills were particularly challenging to fill.

"It is those very technical skills that we are finding tough to recruit at every level. Most of the people coming our way are coming with a visa requirement so we are not seeing UK skills readily available."
(Cyber sector firm,1,000 or more employees)

Similar to the findings from past years, in the qualitative research, penetration testing and cloud security were specific roles that were commonly cited as being hard to recruit.

Complementary and technical skills

In the qualitative research, employers and recruiters highlighted the value of employees who have both technical and complementary skills (sometimes referred to as soft skills). Candidates who combine a strong technical understanding with the ability to engage with non-cyber specialists can be very hard to find – so much so that one employer from a cyber sector firm described them as 'unicorns'.

"What's really tough is to find technical people with consultancy or management consultancy experience. We have recruited a lot of very technical people and we are going to have to work hard over the next 6 to 12 months to develop their soft skills. It is the soft skills in some cases that are more important, can you sit with a client, can you solve a complex problem, can you listen?"
(Cyber sector firm, 1,000 or more employees)

For cyber sector firms, complementary skills allied with technical understanding are especially important for client-facing roles.

However, this skillset is also highly valued in organisations. Employers explained they need people who can engage with and train the rest of the organisation. This was particularly the case for employers with small teams who had broad roles.

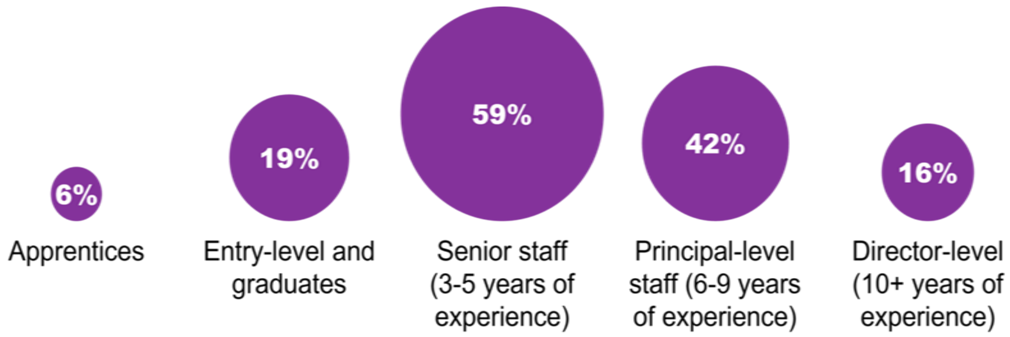
"It's people with the right skills, the ability to think in the right way, the ability to engage, deliver training, all of those things. You need a whole piece because we're so small, we can't afford to subdivide this too much. We can't afford just to have people who are going to just sit and stare at a screen and do analytics. We need people who can engage your staff explain what the problems are, deal with issues, fix stuff."
(Public sector organisation, 250-999 employees)

Specific levels or grades most affected by skills shortages

The bulk of skills shortages are among middle-management and other senior roles, which require 3 or more years of experience (Figure 5.5). These findings are in line with the 2022 and 2021 results. This continues to broadly reflect the findings from the job vacancies analysis (see Chapter 6). This analysis shows that 34% of all cyber jobs identify a minimum requirement of 2 to 3 years' experience and 28% require between 4 to 6 years. It is to be expected that this would be where the majority of hard-to-fill vacancies are as well.

At the same time, it is worth noting that recruitment for positions demanding 6 or more years of experience seems particularly challenging. Over half the employers that have had hard-to-fill vacancies have difficulty finding staff with this high level of experience. By contrast, vacancies at this level make up just 15% of all job postings in the latest data (in Chapter 6), which is consistent with the previous year's study (also 15%). In other words, these higher-level jobs continue to be hard to fill for reasons which go beyond strong demand.

Figure 5.5: Percentage of cyber sector businesses that have found it hard to fill positions at the following levels, among those that have had hard-to-fill vacancies



Base: 79 cyber sector businesses that have had hard-to-fill vacancies in cyber roles since the start of 2021

The qualitative research echoed the quantitative survey findings. Employers and recruiters explained that the middle level of three to ten years' experience level represented the hard-to-fill roles.

"The government has a lot of initiatives to get people into the industry and that will help but we do not have a problem hiring graduates and training them up. The challenge is at that experienced hire level."
(Cyber sector firm, 1,000 or more employees)

Employers valued staff with enough experience and knowledge to handle day-to-day cyber security confidently and also to engage with clients or stakeholders.

"The bit where it is difficult is at the mid-level, people who have 3 to 10 or 12 years' experience. They are the money makers for us. Our customers want experienced people who can do things. They don't want to be paying for graduates! That is a very competitive market, the people with the skills, the badges, the qualifications, and the years of experience. They know what they are worth and it is very competitive. That is where we struggle the most."
(Cyber sector firm, 1,000 or more employees)

One recruiter highlighted that middle level candidates were also probably the only ones within budget for many clients. Although senior director level positions may be challenging to fill, demand is perhaps lower and so the gap less evident. One public sector organisation had found that when they tried to recruit for high level roles, they attracted a lot of inexperienced candidates.

How employers and recruitment agents react to hard-to-fill roles

In the qualitative research, employers said they resorted to the recruitment approaches highlighted earlier in this chapter (section 5.1 on Approaches to recruitment) to recruit for hard-to-fill roles, albeit more aggressively when possible. Recruiters explained that the majority of their candidates were passive and these roles needed a lot of proactive searching and engagement.

Employers said they gave careful consideration to salaries for highly competitive roles, as well as offering benefits such as flexible working.

"Sometimes we have to work with our HR organisation to be clear why that role is at a premium. We'll get feedback from recruitment agents on salary bands and we will use that as evidence and other market information."
(Cyber sector firm, 1,000 or more employees)

Recruiters explained that in some cases employers ran out of options and had to fill the vacancy with someone who did not have the required skills for the role.

"We will often see roles that have been advertised for 6-9 months where they have exhausted all options, tried to hire people directly and it hasn't worked, and they end up compromising – and people without the required skills and capabilities end up in a role they're not qualified to do. That can add to attrition. It's a challenging market to operate in."
(Recruitment agent)

Cyber security job vacancies

This chapter sets out a profile of online cyber security job vacancies. This is based on our analysis of secondary job vacancy data using the Lightcast Analyst platform. It explores the number of job postings, the roles, skills, qualifications, and experience levels in demand, where the demand is coming from (both in terms of economic sectors and geographically) and the salary levels offered. This data focuses on the 2022 calendar year (1st January to 31st December 2022).

Whereas the survey results covered in other chapters are based on a random sample of businesses from the wider population, the charted findings from this secondary analysis are based on the entire dataset of online job postings.

Key findings

- In 2022, there was strong demand for cyber security professionals, with an average of 5,900 core job postings per month from employers. **This is approximately 34% higher than 2021 levels.** However, there may be some evidence that this increase in demand has slowed in the second half of 2022.
- Demand has remained relatively consistent on a regional basis (i.e. growth in demand is occurring across all regions)
- The median advertised salary for core cyber roles in the UK has remained consistent, increasing by just 0.4% from £55,000 in 2021 to £55,200 in 2022. However, this could be due to a greater proportion of employers and recruiters not disclosing salary ranges on job vacancies, as approximately 75% of online core cyber job postings do not contain any salary information, compared to 55% in the previous study.

6.1. Core versus all cyber job roles

The separately published technical report lays out the methodology used for this analysis. The approach is consistent with that of previous years, allowing for an understanding of the changes in the cyber labour market over time. However, Burning Glass Technologies merged with Emsi in 2021, and has since rebranded as Lightcast. This means that the search strategy used previously on the Burning Glass Technologies platform has been rebuilt using the new Lightcast Analyst platform (which uses the same underlying data).

This has been used to undertake two searches (consistent with the 'core' and 'enabled' roles search used in 2021 and 2022 studies). This includes a search for:

- **Core cyber roles** are formally labelled or commonly recognised as cyber security jobs. They have a greater demand for skillsets and tools directly related to cyber security, such as information systems, cryptography, information assurance, network scanners, and security operations. In other words, these are job roles where some aspect of cyber security is the main job function. This would typically include job titles such as Cyber Security Architect, Cyber Security Engineer, Cyber Security Consultant, Security Operations Centre (SOC) Analyst and Penetration Tester

- **All cyber roles** includes the core cyber security roles mentioned previously, in addition to roles that may not formally be labelled or commonly recognised as cyber security jobs, but they still require cyber security skills. Alongside cyber security skills, they demand more general IT and business skills, such as project management, risk assessment, network engineering, SQL, system administration, and technical support. This might be because the job requires light touch knowledge and application of technical cyber security skills (e.g. for IT technicians or governance, regulation and compliance roles) or because the job role includes cyber security functions among other things (e.g. network engineers whose role includes but is broader than just network security). Typical job titles include Computer Support, IT Support Analyst and Applications Analyst

It is worth noting that all of these cyber security job roles typically require a mix of technical and nontechnical cyber security skills. Therefore, these cannot simply be differentiated as technical vs. nontechnical jobs in cyber security.

To be clear, this is a different distinction from the formal versus informal cyber roles discussed in previous chapters, which addresses the fact that most organisations, especially micro businesses, have people carrying out cyber functions on a largely ad hoc or informal basis. By contrast, all the job postings included in this secondary analysis have, by definition, technical aspects of cyber security within their job descriptions. They are all formal cyber roles.

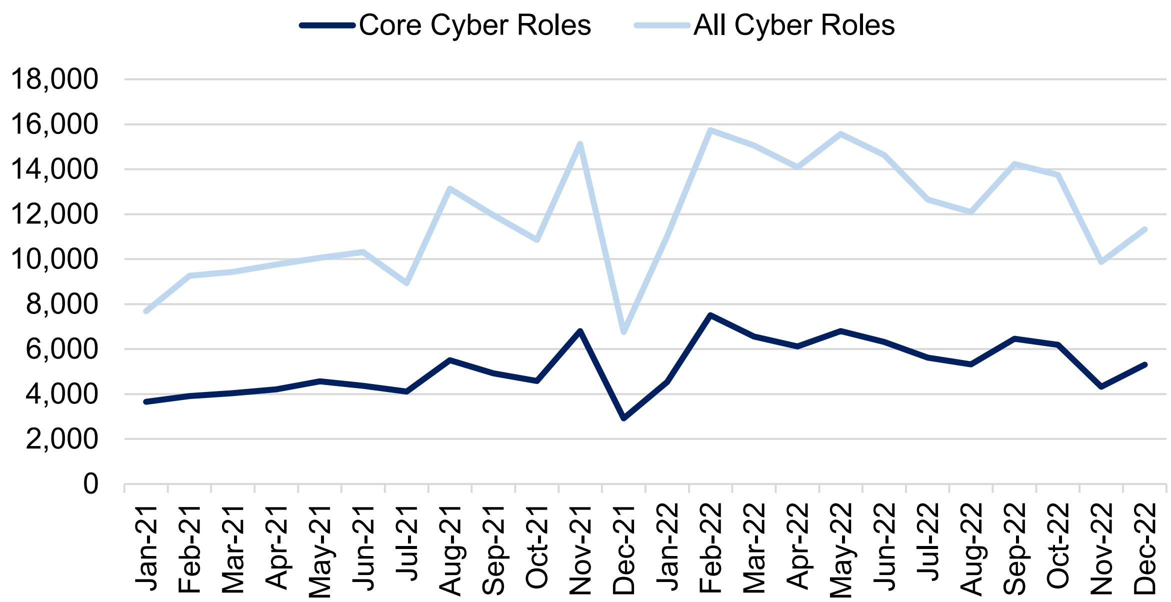
6.2. Number of job postings

The monthly trend for core and all cyber security online job postings is set out in Figure 6.1, spanning the two-year period from January 2021 to December 2022. In the most recent twelve months (i.e. January 2022 to December 2022), there has been strong demand for cyber security professionals.

In 2022, there were 160,035 relevant job postings. This includes 71,054 job postings across core cyber roles (an average of 5,921 per month), and 88,981 other job postings requesting cyber security skills.

When compared to 2021 levels, this suggests that the number of core cyber job postings has increased by 33% (from 53,586 in 2021). Demand for 'all cyber roles' has also increased by 30% in this time period.

Figure 6.1: Monthly number of core and all cyber online job postings from January 2021[9] to December 2022



Source: Lightcast
Bases: 283,318 online job postings from January 2021 to December 2022 (of which 160,035 were in 2022); 124,640 across core cyber (71,054 in 2022).

Figure 6.2 sets out how the volume of cyber security job postings has changed since January 2021. The job postings for each subsequent month are indexed to January 2021, which has an index score of 100. The indices highlight some seasonal drops in demand in both years, however, this drop is expected and is experienced across core cyber vacancies, wider cyber vacancies, and all digital sectors.

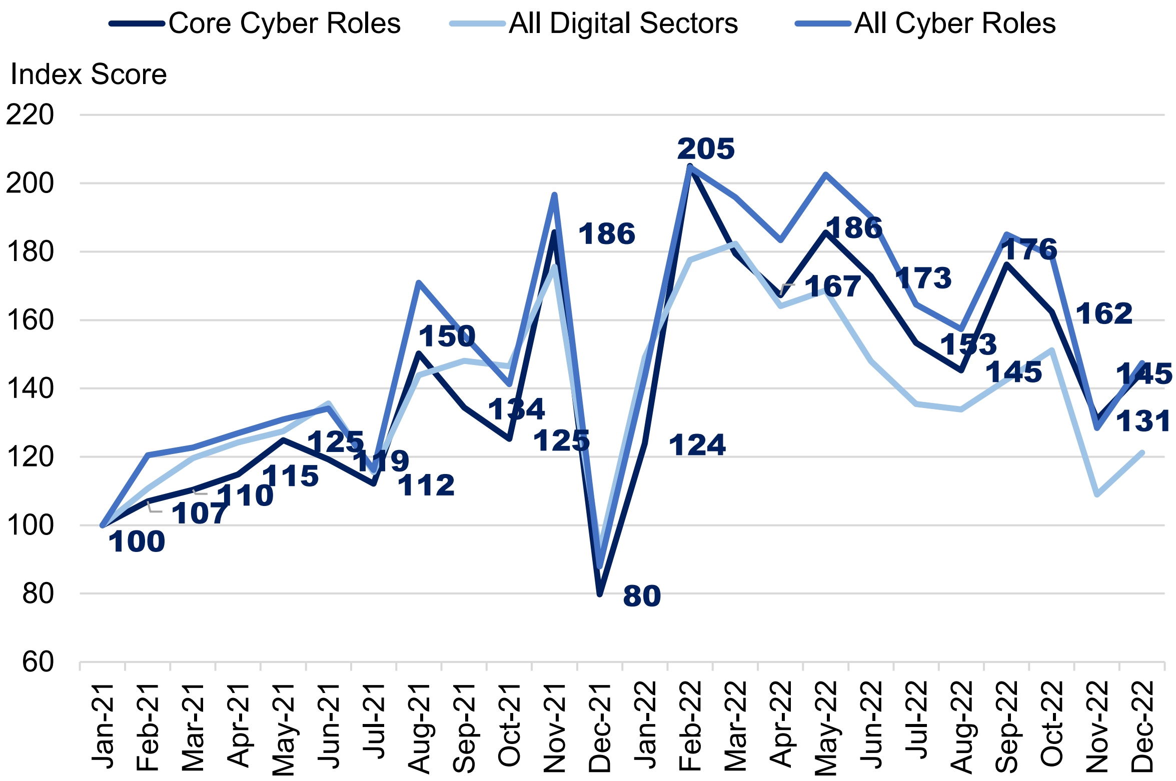
The chart indicates that there has been greater growth in job postings since January 2021 across core cyber roles and all cyber roles than that experienced by all digital sectors. Indeed, demand for cyber

[9] Please note the time series data for 2021 and 2022 in this figure is derived from the updated Lightcast Analyst search. This provides a similar estimate for the number of core cyber vacancies in 2021 (53,591) as the previous Burning Glass Labour Insight tool estimate used in last year's report (53,144) – i.e. the variance is <1%. We do not provide a time series estimate for 'cyber-enabled' roles due to the change in the data tool; however, the use of 'all cyber roles' is considered aligned to this approach.

security professionals grew strongly throughout 2021, and was approximately twice as high in early 2022 than the start of 2021.

However, whilst demand has been high in 2022, the latter half of 2022 suggests that the rate of increase in demand for cyber security professionals may be somewhat slowing. This is also reflected in both charts, as there were 37,851 core postings in H1 2022 compared with 33,203 postings in H2 2022, potentially reflecting a slight slow-down in recruitment activity[10]. However, this demand remains high compared with historic trends.

Figure 6.2: Index of online job postings (January 2021=100)



Source: Lightcast

Bases: 2,727,954 online job postings from January 2021 to December 2022 (of which 1,471,916 were in 2022); 124,640 across core cyber (71,054 in 2022); 283,318 across all cyber (160,035 in 2022); 2,444,636 across all digital sectors (1,311,881 in 2022)

6.3. Geographical differences

The remainder of this chapter focuses on online job postings from January to December 2022 only.

Figure 6.3 shows the proportion of job postings for core cyber roles from each UK region (where region has been provided in the job listing) for 2022. On the heatmap, a darker colour indicates a higher density of cyber jobs in that region. In line with last year's report, the strongest concentration of job posts falls within London and the South East. However, there has been some notable growth in regions such as Scotland (7% from 5.3%), Yorkshire and the Humber (up to 6.8% from 5.6%).

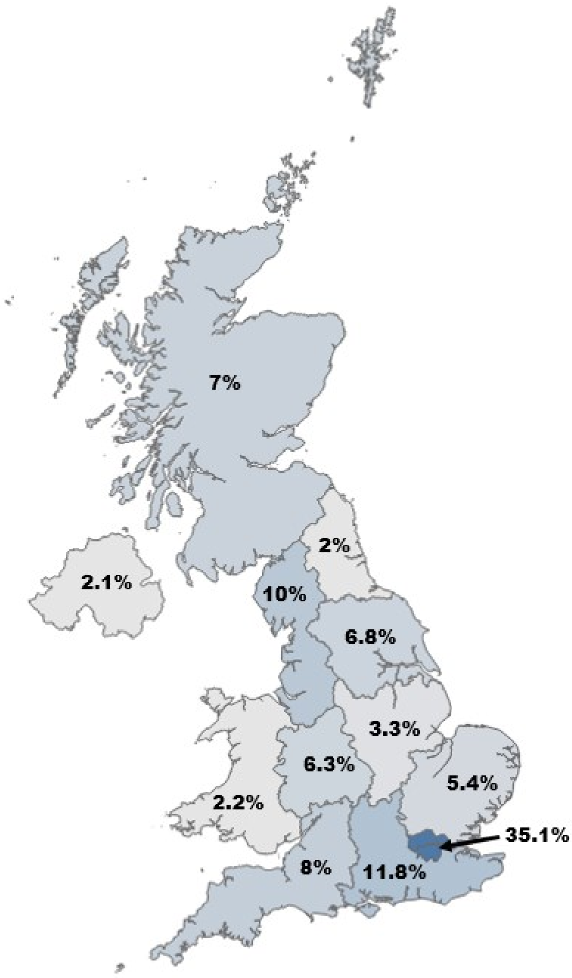
[10] H1 indicates the first half of the year and H2 indicates the second half of the year.

Notably, we estimate that 28% of these postings[11] had no regional location listed (i.e. the roles were marked as 'Remote' or 'UK-wide'). This is an increase from 2021 (21%) and 2020 levels (13%), which suggested an embedded trend towards working from home and remote working across all regions in cyber security.

Figure 6.3: Percentage of core cyber job postings from each UK region (where location is known)

Ranking

1. London (35.1%)
2. South East (11.8%)
3. North West (10%)
4. South West (8%)
5. Scotland (7%)
6. Yorkshire and The Humber (6.8%)
7. West Midlands (6.3%)
8. East of England (5.4%
9. East Midlands (3.3%)
10. Wales (2.2%)
11. Northern Ireland (2.1%)
12. North East (2%)



Source: Lightcast
Base: 50,951 online job postings with location data from January 2022 to December 2022

Figure 6.4 sets out the top cities by number of core cyber job postings alongside the heatmap that highlights the top fifteen UK local authorities in terms of Location Quotient rankings.[12]

The top five cities by number of absolute job postings have remained consistent from 2021, with Greater London, Manchester, Bristol, Birmingham, and Leeds having the highest number of cyber security job postings.

[11] Of the 71,054 job postings, 20,103 (38%) did not have a known regional location.

[12] The Location Quotients are calculated using the total workforce jobs for a local authority region. The average demand is set at 1.0. A higher Location Quotient indicates that the demand for core cyber employees is higher than the UK average. Please note The data within this year's report is available for Local Authority level, and not Travel to Work Area as used in previous reports.

In terms of Location Quotient ranking by workforce jobs, Cambridge is the top for cyber security job postings. Some of the highest demand areas include Reading, Bristol, and Manchester. In 2022, there has also been strong demand in areas such as Guildford, Cheltenham, Oxford, and Belfast.

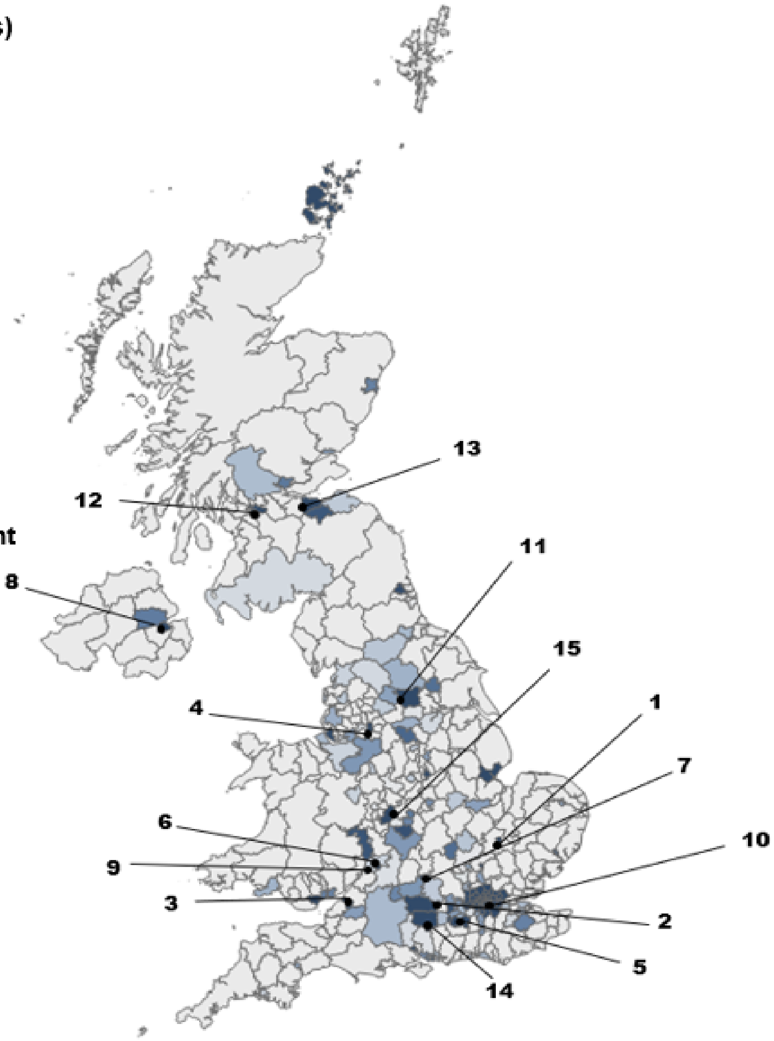
Figure 6.4: Number of core cyber job postings and Location Quotients in the top 15 UK Local Authorities

Top 15 in terms of absolute number of job postings (number in brackets)

1 – Greater London (17,984)
2 – Manchester (2,707)
3 – City of Bristol (2,303)
4 – Birmingham (1,550)
5 – Leeds (1546)
6 – Glasgow City (1,299)
7 – City of Edinburgh (1,089)
8 – Reading (914)
9 – Cambridge (909)
10 – Belfast (859)
11 – Liverpool (673)
12 – Cardiff (601)
13 – Nottingham (557)
14 – Sheffield (530)
15 – Newcastle upon Tyne (473)

Top 15 in terms of Location Quotient (shown in brackets) with ranking labelled on map

1 – Cambridge (5.07)
2 – Reading (5.01)
3 – City of Bristol (4.88)
4 – Manchester (4.03)
5 – Guildford (2.57)
6 – Cheltenham (2.52)
7 – Oxford (2.33)
8 – Belfast (2.28)
9 – Gloucester (2.26)
10 – Greater London (2.07)
11 – Leeds (2.03)
12 – Glasgow City (1.91)
13 – City of Edinburgh (1.89)
14 – Basingstoke and Deane (1.84)
15 – Birmingham (1.80)



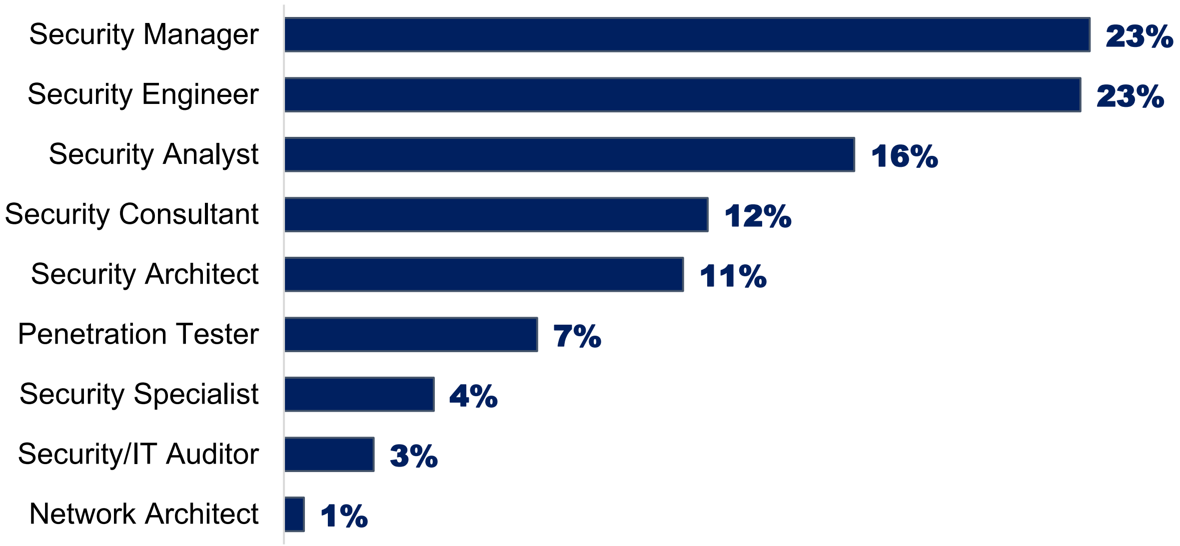
Source: Lightcast
Base: 50,551 online job postings with local authority location data from January 2022 to December 2022

6.4. The job roles being advertised

Figure 6.5 lists the identified core cyber roles by job title. Vacancy data can contain several variations of similar titles (e.g. Cyber Security Analyst, and Cyber Analyst), and therefore, as with previous years, minor variations in roles have been combined.[13]

[13] We have categorised the top 50 job titles appearing in the data. This covers 29,289 of the total 71,054 core job postings for the latest 12-month period. We have categorised the top 50 into key cyber job titles, and wider review of the data suggests that Figure 7.5 is considered to be representative of wider job titles for cyber security roles.

Figure 6.5: Top recurring job titles among the core cyber job roles identified



Source: Lightcast
Base: 29,289 online job core cyber job postings from January 2022 to December 2022 featuring one of the top 50 job titles (across 71,054 core cyber job postings).

The five most demanded roles have remained consistent with 2021, however, with some changes in relative proportion. Security Manager job postings have increased from 14% of roles to 23% of roles in 2022. The proportion of Security Engineer postings has decreased, from 35% in 2021 to 23% in 2022.

This may suggest some increased demand for cyber security professionals within mid-level management roles, particularly within domains such as consultancy, professional services, finance, and public sector, as explored subsequently in Section 6.5. However, many of these roles will have complementary skillsets, and may reflect how employers and recruiters are defining and categorising roles.

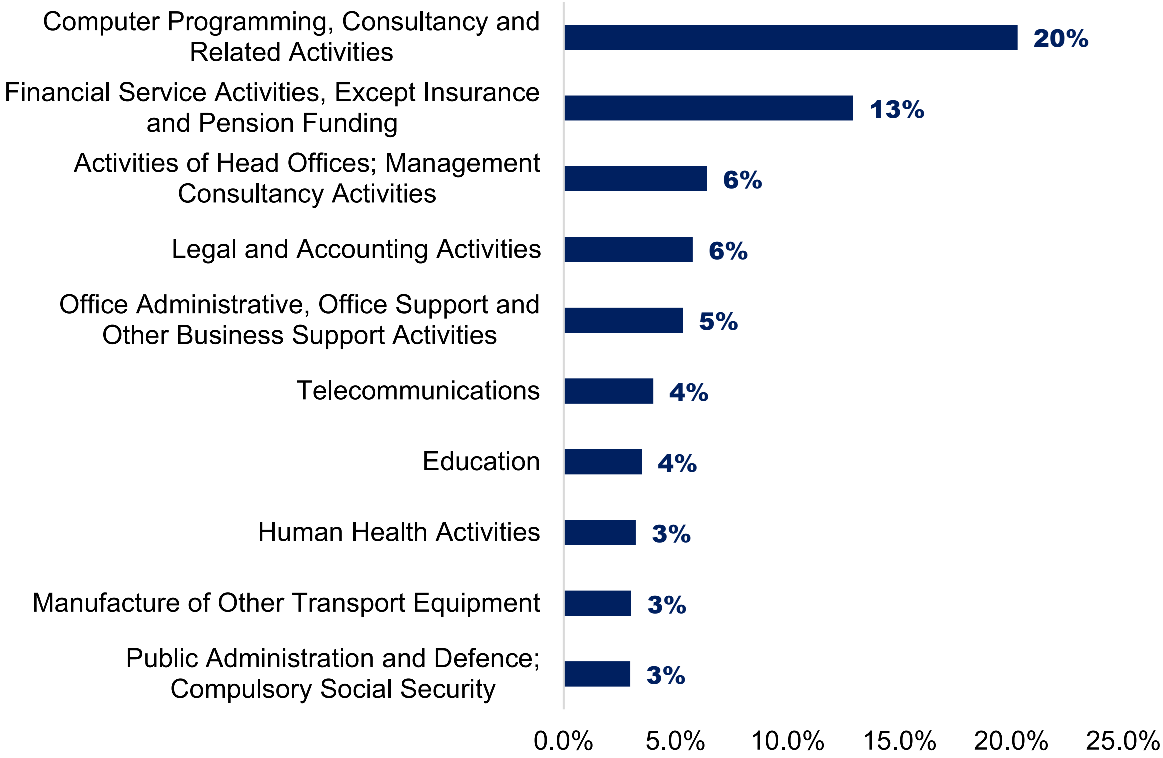
6.5. The sectors demanding cyber security staff

Job postings within the dataset are typically advertised through a recruitment agency, with almost half of roles in the dataset linked to recruiters. However, for those roles with a named employer, the data suggests the following sectoral breakdown.

This is not necessarily a comprehensive breakdown. As noted earlier in this chapter, the Lightcast dataset is liable to omit some key large employers that do not post job adverts directly.

The following sets out the sectors with the highest demand for core cyber roles in 2022. It is important to note that greater than 20,000 core cyber roles were posted by recruitment agencies, suggesting a demand among employers to use recruiters. Consequently, the following looks at the top sectors for core cyber postings, excluding employment activities.

Figure 6.6: Percentage of job adverts for core cyber roles coming from specific sectors (where the employer is named)



Source: Lightcast

Base: 25,378 core cyber job postings with sector data from January to December 2022 (excluding recruitment agency postings).[14]

Further exploration of the key employers of core cyber roles highlights that there is significant demand among public sector (e.g. GCHQ, NHS), professional services and finance (e.g. PwC, Deloitte, Barclays, KPMG, EY), telecommunications (e.g. BT, Vodafone), and aerospace and defence (e.g. BAE Systems).

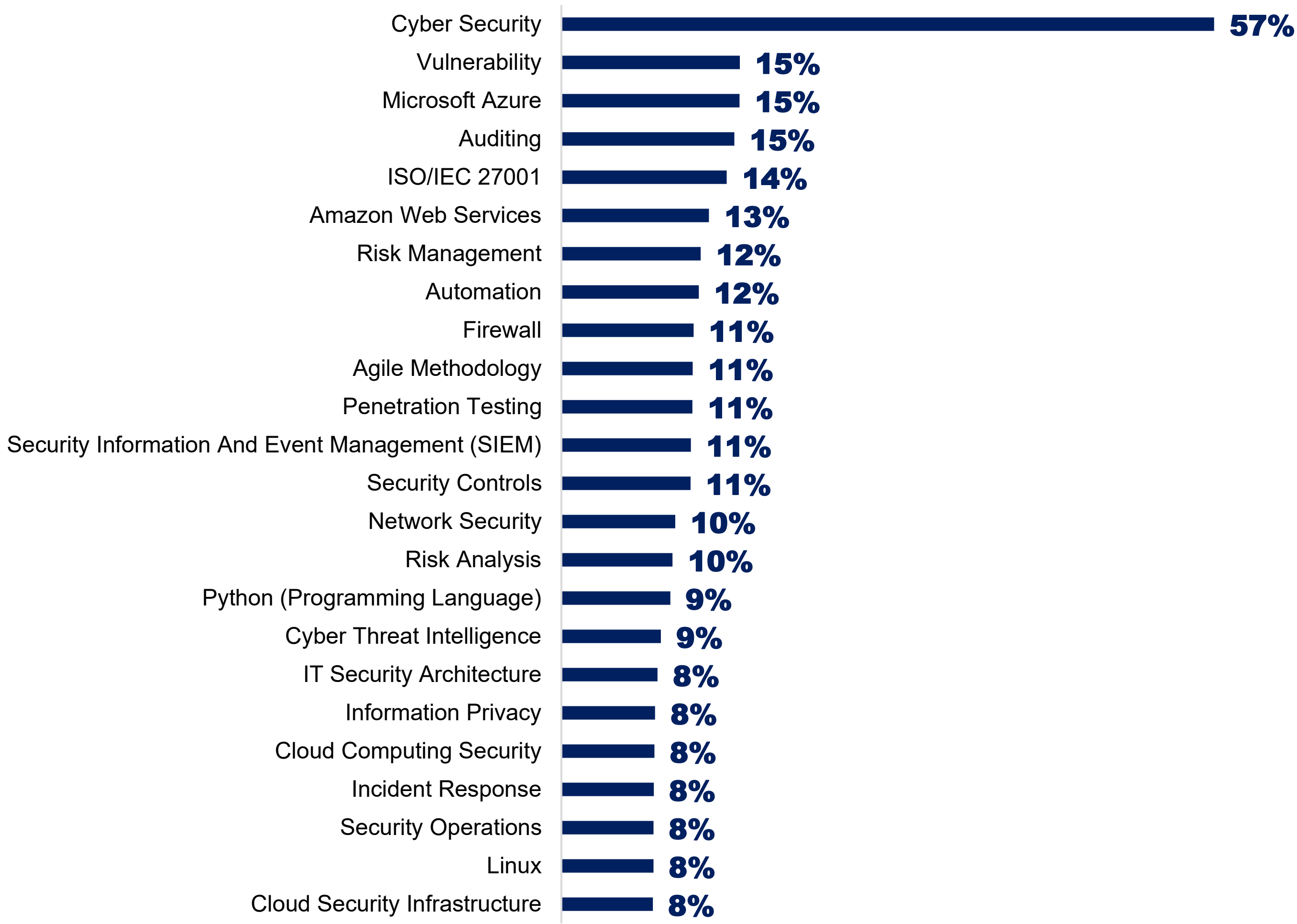
[14] Human health activities typically refer to the health and social care sector – the NHS is the largest employer of cyber security roles within this sector.

6.6. The skills, qualifications and experience being demanded

Skills in demand

There has been no major change in the type of skills being demanded for core cyber roles compared to last year. The top three technical skills requirements mentioned in job descriptions are cyber security skills, vulnerability, and Microsoft Azure. Other sought-after skills areas include network engineering, risk management and technical controls, knowledge of operating systems and virtualisation, cryptography, and programming (e.g. Python). Figure 6.7 sets out some of the top requested skills.

Figure 6.7: Top skills requested for core cyber job roles



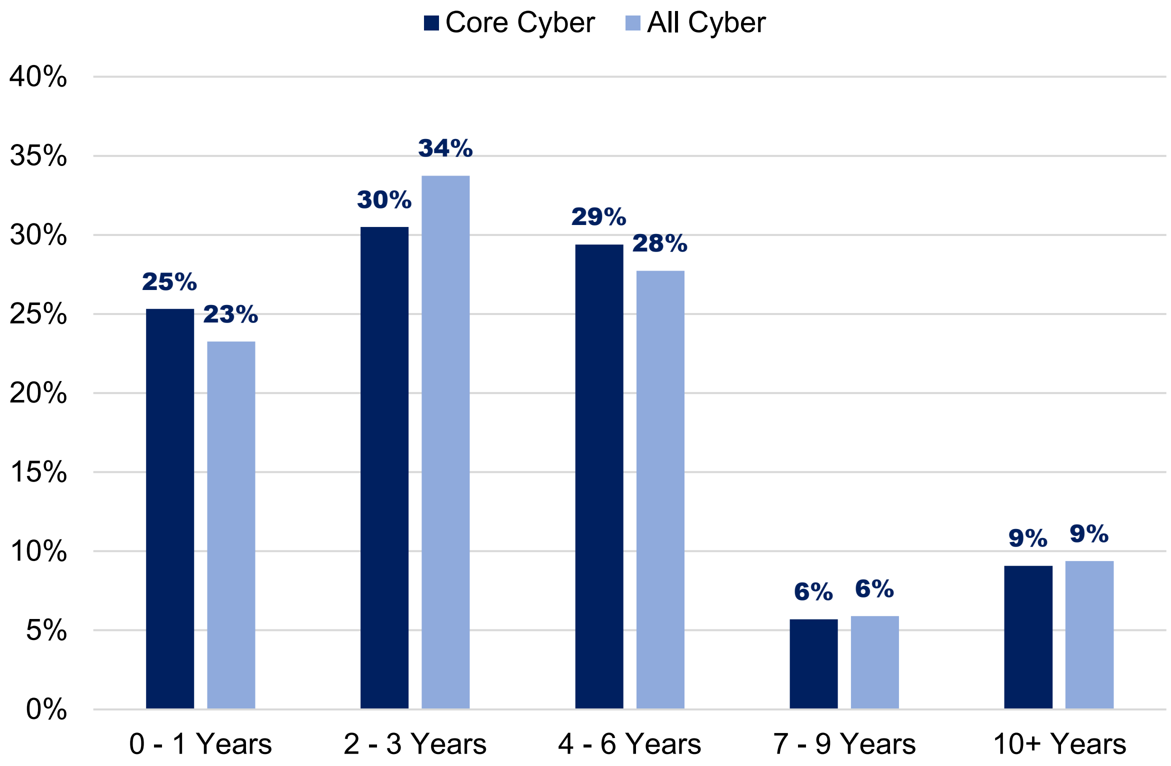
Source: Lightcast
Base: 71,054 core cyber job postings from January to December 2022 that have at least one skill listed.

Experience requirements

Figure 6.8 demonstrates that, over the last year, the most common request from employers looking to fill core cyber security roles has been for applicants with mid-level experience (2-6 years, 59%), followed by entry-level applicants (25%).

This preference for mid-level experience is in line with the previous study.

Figure 6.8: Percentage of core and all cyber job postings asking for the following levels of minimum experience (where any minimum requirement is identified)

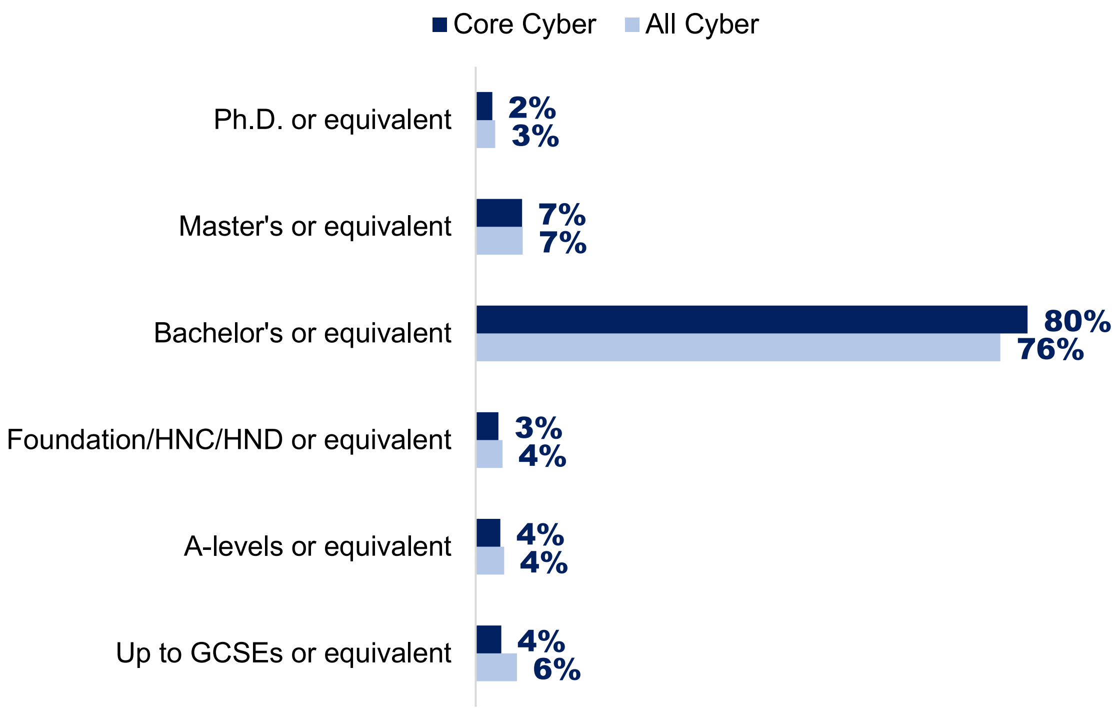


Source: Lightcast
Base: job postings from January to December 2022 that have specific experience listed: 18,985 core cyber job postings; 43,083 all cyber job postings

Education requirements

Figure 6.9 sets out minimum education requirements that employers are looking for in core and wider cyber job postings. The results show that 80% of core cyber employers require applicants to have a minimum of a bachelor’s degree (or equivalent), with a further 9% wanting postgraduate qualifications such as a master's degree or PhD. The proportional share of requirements for wider cyber roles is similar, with almost 90% of employers looking for candidates with a bachelor’s or higher degree.

Figure 6.9: Percentage of core and all cyber job postings asking for the following levels of minimum education (where any minimum requirement is identified)



Bases: Job postings with minimum experience listed from January 2022 to December 2022; 14,481 across core cyber; 32,837 across all cyber
Source: Lightcast

Assessing candidate proficiency

In the qualitative interviews, although qualifications and certifications were important, particularly for more technical roles, employers often placed greater value on experience and exposure to systems, software, incidents, and threats. The length of experience employers were looking for could vary by role. Examples given were requiring between one to five years' experience for ethical hackers but at least three to five years for more senior management roles.

"We do look at qualifications but we look at who they are and what their experience is 90% and qualifications are the icing on the cake."
(Cyber sector firm, 1,000 or more employees)

However, qualifications and certifications could play an important role in assessing candidates' ability and knowledge.

"We obviously look at degrees but typically we find industry certifications to be more of a marker of ability than degree. That's purely because they seem to be more specialised. Degrees seem to cover a lot but not with particular depth."
(Recruitment agent)

Qualifications are particularly valued in certain roles, for instance, Certified Ethical Hacker (CH/CEH) for ethical hackers.

“With [security and incidence] role you do want the high-level security certifications. It gives us comfort; it gives our cyber insurers comfort as well. That was a relatively non-negotiable requirement. If we don’t have certified people, then we have to have cover at a lower level.”
(Private sector organisation, 250-999 employees)

While some employers sought candidates with degrees, most obviously for graduate entry programmes, others felt degrees were less relevant in evaluating candidates.

"From my perspective we tend to judge proficiency in terms of experience or potential rather than formal qualifications. For instance, when we have offered entry-level roles we didn’t require candidates to have an IT degree, we focused more on the enthusiasm they demonstrated through their application and interview. For more senior level roles, we much prefer to look at a candidate’s experience and professional on-job qualifications, rather than formal qualifications."
(Public sector organisation, 250-999 employees)

Employers generally assessed candidates on their attitude, especially for more entry level roles where they wanted to understand whether there was drive and desire to grow into the role offered.

The key traits employers were looking for included enthusiasm, curiosity, problem-solving, and mental agility. A desire to learn was also valued, particularly where candidates did not currently meet all of the requirements of the role.

“We try not to be too distracted by that [qualifications]. It is more the aptitude of the person and whether they will fit in the team. The certifications are a nice to have but we can invest in people if we need them to have the certifications. It comes back to diversity and inclusion. If you start to say that people have to have certain certifications, then you close yourself out of the marketplace.”
(Cyber sector firm, 1,000 or more employees)

Employers also usually evaluated complementary skills during interviews. These could include communications, project management, business development, and client management depending on the role. This was to understand the candidate’s ability to work effectively with clients or other non-cyber teams.

Candidates’ proficiency was typically evaluated in interviews (which could be two-stage). A few cyber sector firms had streamlined their approach as they could not afford to lose candidates because they had not moved quickly enough.

6.7. Salaries

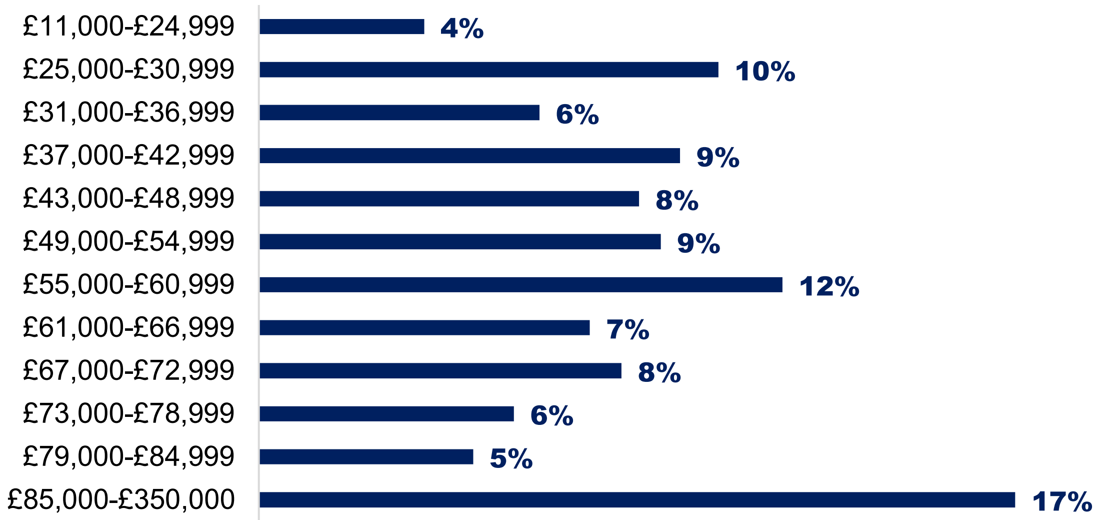
Using the Lightcast Analyst platform, we estimate the mean salaries by averaging the midpoints of the advertised salaries and the number of observations. Across the 12 months of 2022, the average (mean) advertised salary was £59,400 for a core cyber job posting (with a median value of £55,200). Please note due to the updated platform, we do not provide a full time series analysis.

As a comparison, for all employee jobs within Standard Industry Classification (SIC) 2007 code 62, which is the computer programming, consultancy and related activities industry code, the mean annual pay increased by 0.5% from £48,369 in 2021 to £48,600 in 2022 (with median increase of 5% from £40,000 in 2021 to £42,000 in 2022)[15].

Using this value as a proxy for IT jobs in the UK suggests there is a wage premium of approximately 33% for core cyber security jobs compared to IT jobs (when comparing median salaries).[16] Figure 6.10 sets out the percentage of core cyber roles offering salaries within the following ranges, where the salary is advertised.

It is also worth noting that around 75% of online core cyber job postings do not contain any salary information, compared to 55% last year. This may suggest there has been a reduction in salary transparency for cyber security roles, or that there is an increase in the use of recruitment agencies and therefore, undisclosed salaries on job adverts.

Figure 6.10: Percentage of core cyber job postings offering the following salaries (where salary or salary range is advertised)



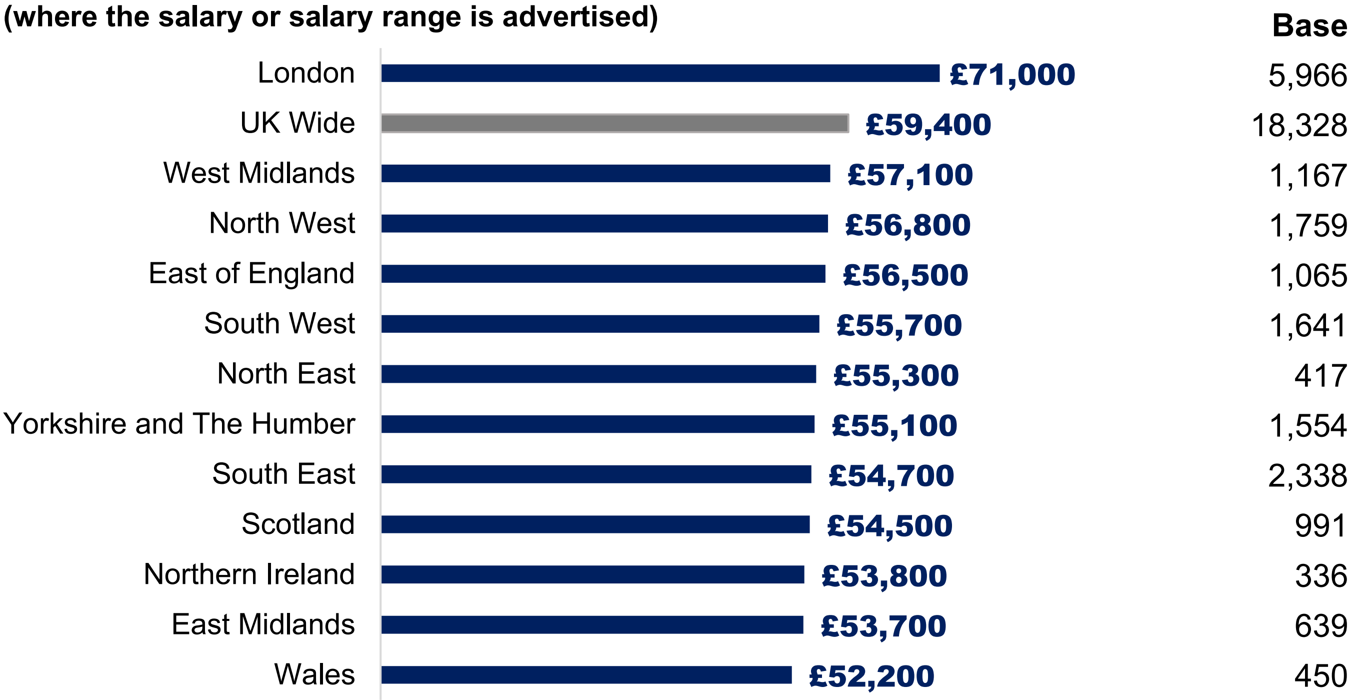
Source: Lightcast
Base: 18,326 core cyber online job postings with salary data that can be mapped to a specific UK region from January 2022 to December 2022 (the remainder are based in the UK but may include national or remote locations)

[15] This is sourced from the Office for National Statistics (ONS, 2022 provisional data) [Annual Survey of Hours and Earnings.](#)
[16] Comparing the 2022 median for core cyber job postings (£56,000) with the 2022 median for all IT postings (defined as SIC 62, getting a provisional median of £42,000)

Geographical variations in salaries

London has the highest mean advertised salary for core cyber roles, and is consistently ahead of other regions, as shown in Figure 6.11. Whilst there is variation in salaries across regions, pay disparity across regions appears lower than previous years (i.e. £23,200 difference between highest and lowest region in 2021 compared to £18,800 in 2022).

Figure 6.11: Mean salary offers for core cyber job postings, by region (where the salary or salary range is advertised)



Source: Lightcast
Base: 18,328 core cyber online job postings with salary data that can be mapped to a specific UK region from January 2022 to December 2022 (the remainder are based in the UK but may include national or remote locations)

Staff turnover in the cyber sector

This chapter measures staff turnover within the cyber sector and the reasons why staff have left their posts (where employers are aware of the reason). These statistics were included for the first time in the 2021 report. In keeping with last year, the timeframe captured in these statistics is the last 18 months before the survey, which this time approximately equates to the start of January 2021.

Key findings

- A total of 11% of the cyber workforce (within the cyber sector) are estimated to have left their posts since the start of 2021, with 9% leaving of their own volition. These figures are the same as last year.
- The company offer not being good enough (61%) has overtaken uncompetitive pay or benefits (51%) as the most common reason employers give for staff leaving of their own volition

7.1. An estimate of cyber workforce staff turnover

We estimate that 11% of the cyber workforce (within the cyber sector) left their posts in the 18 months prior to the survey (i.e. since around January 2021). This is a bare minimum estimate, as the size of the total workforce in our calculations assumes, for simplicity, that all these staff were all in post 18 months ago (i.e. they did not join and leave within the last 18 months, which is possible).

This turnover rate is the same as the previous year's estimate (also 11%).

In the qualitative research, employers said that the staff leaving tended to be at the mid-level of seniority. Employers were losing staff in technical roles that are generally hard to recruit, such as security architects. This was a reflection of the high demand for these roles:

"We lost two people recently [working in cloud security] which was a real blow to us. The market is so hot, they were offered crazy packages."
(Cyber sector firm, 1,000 or more employees)

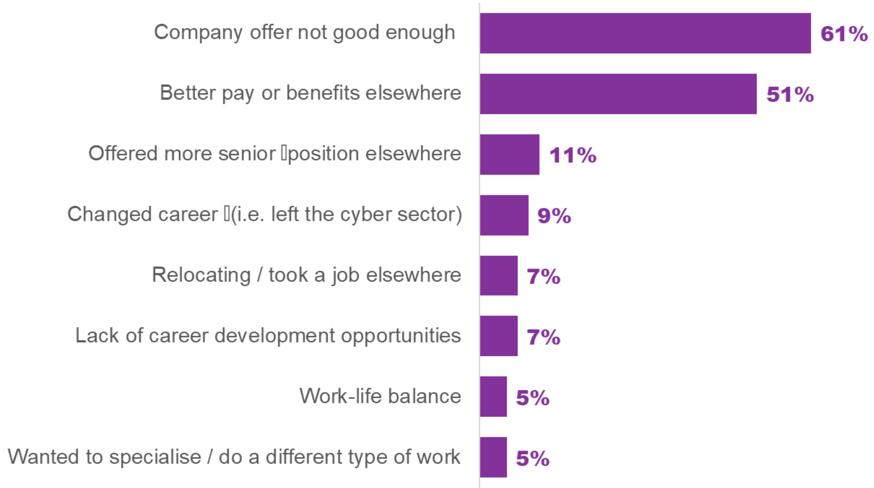
7.2. Why employees leave their roles

A total of 9% left of their own volition, with the remaining 2% leaving due to either dismissal or redundancy. This is consistent with the previous study where 9% left of their own volition and 2% were dismissed.

In the 9% of cases where staff left of their own volition, we asked employers about the reasons behind this. It is important to note that this data, shown in Figure 7.1, covers employers' *perceptions* of why these employees left their posts, which may be different from employees' own views.

The most common reason offered by employers is that staff left because the company offer was not good enough. This is a change from last year where the most common reason offered by employers as to why staff left was to getter better pay or benefits elsewhere.

Figure 7.1: Reasons employers give for staff leaving cyber job roles, among those where any employees left of their own volition (unprompted – multiple answers allowed)



In the qualitative research, employers explained that a combination of factors – which equates to the overall company offer – caused staff to leave. Salary was a key reason but opportunities to develop skills, career progression, and to do more interesting work were other motivations.

"The things that were drawing them away from us were things that we couldn't necessarily compete with. We couldn't compete with the salaries. We couldn't compete with the excitement level of the new roles as well. We're talking a leapfrog from us to big corporate household names and exciting opportunities."
(Cyber sector firm, 10-49 employees)

Another factor highlighted in the qualitative research was achieving promotion. This was expected in large cyber sector businesses where staff can get a bigger jump in both salary and promotion if they went to a competitor.

In the qualitative research, both employers and recruitment agents thought that the public sector was particularly vulnerable to losing employees because of pay. Recruitment agents said that public sector candidates could be very sought after because they were well trained and cheap relative to others, while the candidate themselves could achieve a significant rise in pay.

"About a year ago, we had someone who was just trained, and they then left because the other organisation paid them a lot more money than we are offering. And it has taken almost a year to recruit that post."
(Public sector organisation, 250-999 employees)

Recruitment agents noted that some private sector companies could offer large bonuses, equity packages, and good benefits. Both recruitment agents and employers highlighted that large tech firms were particularly likely to offer high salaries to candidates.

In the qualitative research, we found that this was a particular issue for public sector organisations which have few or no senior roles and therefore little opportunity to progress. A related issue for all employers is offering limited or no opportunities to develop skills. This could be due to a lack of training budgets or the types of services they offer or a combination of the two.

The proportion saying that employees had left because of work life balance remained broadly similar (6% in 2022 and 5% this year). In the qualitative research, some cyber sector employers highlighted that burnout from long hours and highly pressurised work were reasons why some staff left. Recruitment agents identified this, along with salary, as a key reason why people left large private sector organisations.

"Elsewhere you can get more money for less work. One guy said he was working Saturday morning so he wasn't drowned when he came in on Monday."
(Cyber sector firm, 50-249 employees)

Only a minority of employers said that staff left to a change of career (9%). This echoes what was found in the qualitative research, where only one cyber sector firm reported staff leaving the sector altogether. This was attributed to the exhausting and stressful nature of the work their staff experienced.

7.3. Retention strategies and future turnover

Retention strategies

In the qualitative research, we asked employers what strategies they had in place to retain cyber staff. A few had no specific approaches as such or were philosophical about employees leaving.

A couple of public sector organisations we spoke to focused their efforts on growing talent through apprenticeship programmes rather than retention.

“What we want to do is to invest more into the kind of apprenticeship programs where we can grow our own, produce them in an environment where they understand the peculiar oddities of local government and that the risks that we've got are not exactly the same as the private sector. And then bring them through into those roles so that we've got people ready to go as positions free up.”
(Public sector organisation, 250-999 employees)

Employers who did have strategies to hold onto cyber staff talked about offering staff opportunities to progress, to develop their skills and to do interesting work. This development could involve training to achieve certifications or the chance to learn new skills, for instance in a new technology or leadership roles.

“People need to believe that there is progression and see it happening. It is what comes up when people do leave, that is usually part of the conversation. They have lost sight of what their next

step is sometimes. You have to give people a really clear idea of that."
(Cyber sector firm, 1,000 or more employees)

However, employers highlighted that providing training and the opportunity to achieve qualifications carried the risk that employees then leave because they have become more valuable in the marketplace. A private sector organisation had twice trained someone to take on a dedicated cyber role but both times that person quickly left. As shown in the quantitative findings in Chapter 5, a lack of technical skills/knowledge is the most common reason offered by cyber sector businesses for having a hard-to-fill vacancy (44%). Candidates with relevant qualifications are therefore sought after.

The risk of staff leaving after obtaining qualifications was regarded as particularly acute in hard-to-fill roles like cloud security. One cyber sector business reported training people up on cloud security and then losing them because they were offered double the salary.

Employers also talked about ensuring their organisation is a good place to work. This encompassed organisational culture, good team working, managing workload, and social events. A couple saw offering hybrid working as an important factor here. Large cyber firms looked to give staff at least some say in what they worked on.

Employers saw salary as less of a lever to keep staff but thought it was important to pay employees market rates. A couple had reviewed salaries and increased pay as a result. One medium sized cyber sector business had given staff a lump sum payment to help with the cost-of-living crisis. Some employers highlighted the role of career progression and promotions in increasing an individual's salary.

"You give people new opportunities and the ability to increase their experience, and you make sure you've got the best tools. You have to pay market rates but you also have to make sure that people enjoy where they are working."
(Private sector organisation, 250-999 employees)

Future turnover

The staff which employers were most concerned about losing in the future are those with the technical skills which are already hard to retain. Some employers highlighted that the continuing shift to cloud platforms would mean that demand for these particular skills would increase even further. People with specific experience of major platforms such as in Microsoft or Amazon Web Services would be particularly sought after.

"With clients moving to the big public cloud platforms, those security architecture and engineering experienced people are the people that we will massively need over the next 5 to 10 years and there is so much competition for them. With that skillset, we are competing with Google and Facebook and Amazon and Microsoft. It's really hard."
(Cyber sector firm, 1,000 or more employees)

Some employers also felt that risk and compliance roles were going to grow in importance because businesses were likely to take cyber security more seriously in the future.

The supply of cyber security skills

This chapter explores the supply of cyber security skills within the UK. It draws upon the methodologies used in the previous Cyber Skills in the UK Labour Market (2022) research and the UK Cyber Security Recruitment Pool research. These reports estimated the size of the UK cyber security workforce and the upcoming recruitment pool, based on a review of existing literature and wide range of labour market datasets.

In addition, this strand provides statistics on the estimated characteristics of the cyber security recruitment pool in terms of demography, diversity, location, education, earnings and entry to the cyber security workforce. It also explores routes into cyber security, including higher and further education, apprenticeships, and retraining and reskilling initiatives.

This chapter provides an update to the previous research, using most recent data where available.

Key findings

- For 2022, we estimate the UK cyber security workforce to be in the region of 133,400 individuals. The 2021 estimate was c.131,000. This suggests there has been no substantial change in the total size of the workforce since last year
- A total of c.7,000 individuals entered the cyber security workforce in 2022, which is similar to the 2021 inflow.
- In the most recent available year (2020/21), the number of students enrolled in cyber security courses has increased by 29% (from 14,910 to 19,200) and the number of students graduating in a cyber security course has also increased by 19% (from 3,670 to 4,360).
- We estimate that 3.5 per cent of the cyber security workforce left the profession entirely in 2022. This suggests an estimated outflow of c.4,600 leavers per year
- Employment in the cyber security sector has increased by 10% within the last year. This suggests a need for 13,500 new people each year to meet demand, in addition to the c.4,600 to replace those exiting the sector, i.e. a total requirement of c.18,200 per year
- Taken together, these findings suggest a net annual shortfall of c.11,200 people in 2022.

8.1. The role of higher education

This section focuses on the latest data on graduate enrolments outcomes from the Higher Education Statistics Authority (HESA) and Jisc. The research team made a bespoke data request for cyber security and computer science enrolments and outcomes covering up to the academic year 2020/21 (most recent available).

UK Higher Education provides a considerable range of courses, modules, and opportunities to explore cyber security at both undergraduate and postgraduate level. As the demand for cyber security professionals has grown in recent years, the Higher Education sector has responded through the provision of:

- Dedicated cyber security courses (in cyber security or digital forensics)
- General computer science or computing courses with one or more modules in cyber security
- Non-technical courses with modules in cyber security (e.g. cybercrime modules in psychology)

The National Cyber Security Centre (NCSC) has certified several of these degrees at Bachelor's and Master's level under the NCSC-certified degrees programme. It has also supported the development of Academic Centres of Excellence in Cyber Security Research (ACE-CSR) and Academic Centres of Excellence in Cyber Security Education (ACE-CSE).

Key findings (supply)

- There has been a 29% increase from the 2019/20 to 2020/21 academic year in the number of students enrolled in cyber security courses at undergraduate and postgraduate level.
- This has accompanied a 19% increase in the number of cyber security graduates over the same academic years.

- The gender gap for cyber security courses remains persistent, with only 12% of graduates at undergraduate level, and 23% at postgraduate level identifying as female. For enrolled students, this is similar at 13% of undergraduate students, and 23% of postgraduate students.
- The number of non-EU students has increased. This is particularly pronounced at postgraduate level, with 45% of students from a non-EU background.

- The analysis of graduate earnings suggests a strong entry-level median salary for graduates in cyber security professional roles (approximately £30,000 to £35,000 per annum) in the most recent year.

Courses

Table 8.1 shows the number of courses provided by UK Higher Education Institutions in cyber security and computer science (based on unique course titles offered in 2019/20 and 2020/21).

Table 8.1: Number of cyber security and computer science courses and providers (2019/20 and 2020/21 academic years)

Qualification Level	Cyber Security	Computer Science
Undergraduate	296 (from 70 universities)	2,407 (from 126 universities)
Other UG	10 (from 9 universities)	210 (from 59 universities)
Postgraduate	251 (from 80 universities)	2,074 (from 125 universities)
Total	**557**	**4,691**

Source: Analysis of Jisc / HESA data (2019 – 2021)

This identifies 70 universities providing cyber security undergraduate courses, and 80 universities providing cyber security postgraduate courses in the UK. This is a small increase from 66 and 76 universities respectively in last year's report. Further, the number of cyber security related courses offered has increased by 16% (from 482 to 557).

The number of universities providing computer science courses has stayed relatively level, however, the number of undergraduate and postgraduate courses have also increased by 23% (from 3,818 to 4,691).

In line with this increased provision, demand for studying cyber security and computer science has also increased in the previous year. Tables 8.2 and 8.3 provide updated figures (from the previous cyber skills research) for student enrolment and graduates in both cyber security and computer science courses for 2020/21.

Table 8.2 shows an increase of 29% in the number of students enrolled in cyber security courses from 2019/20 to 2020/21, while Table 8.3 shows an increase of 16% in the number enrolled in computer science courses. The tables also show that the number of cyber security and computer science graduates have grown by 19% and 18% respectively. This highlights relatively strong growth in cyber security provision at both undergraduate and postgraduate levels, indicating that many higher education institutions are responding to the increasing demand for cyber security professionals in the economy, as well as increased demand among students to learn cyber security skills.

Table 8.2: Breakdown of student enrolment and qualifiers in cyber security courses in UK Higher Education institutions (HEIs, 2019/20 and 2020/21 academic years)

	Number of HEIs offering a relevant course		**Number of students enrolled**			**Number graduating**	
Academic Year	2019/20	2020/21	2019/20	2020/21	Increase	2019/20	2020/21
Undergraduate	66	69	10,200	12,990	+2,790	2,200	2,590
Postgraduate	76	68	4,710	6,210	+1,500	1,470	1,770
Total	**85**	**93**	**14,910**	**19,200**	**+4,290 (+29%)**	**3,670**	**4,360 (+19%)**

Source: Analysis of Jisc / HESA data (2019 – 2021) (numbers are rounded to the nearest ten, may not sum due to rounding)

Table 8.3: Breakdown of student enrolment and qualifiers in computer science courses in UK Higher Education institutions (HEIs, 2019/20 and 2020/21 academic years)

	Number of HEIs offering a relevant course		**Number of students enrolled**		**Number graduating**	
Academic Year	2019/20	2020/21	2019/20	2020/21	2019/20	2020/21
Undergraduate	126	128	98,970	106,820	21,630	24,310
Postgraduate	124	124	38,550	52,310	11,600	14,800
Total	**131**	**132**	**137,520**	**159,130 (+16%)**	**33,230**	**39,110 (+18%)**

Source: Analysis of Jisc / HESA data (2019 – 2021) (numbers are rounded to the nearest 10/ May not sum due to rounding.)

These tables show that, in the most recent available year (2020/21), the number of individuals enrolled in cyber security courses has increased by 29% and the number of cyber security graduates has increased by 19%.

Furthermore, computer science enrolments have also increased by 16%, and the number of computer science graduates has increased by 18%. This increase is welcome in the medium-to-longer term, as the proportional growth of graduates (c.19%) is stronger than industry growth levels (c. 10% per annum).

However, this is still from a relatively low base (in the thousands across the country), and therefore will be only one inflow among others such as reskilling and apprenticeships in tackling the UK cyber skills gap.

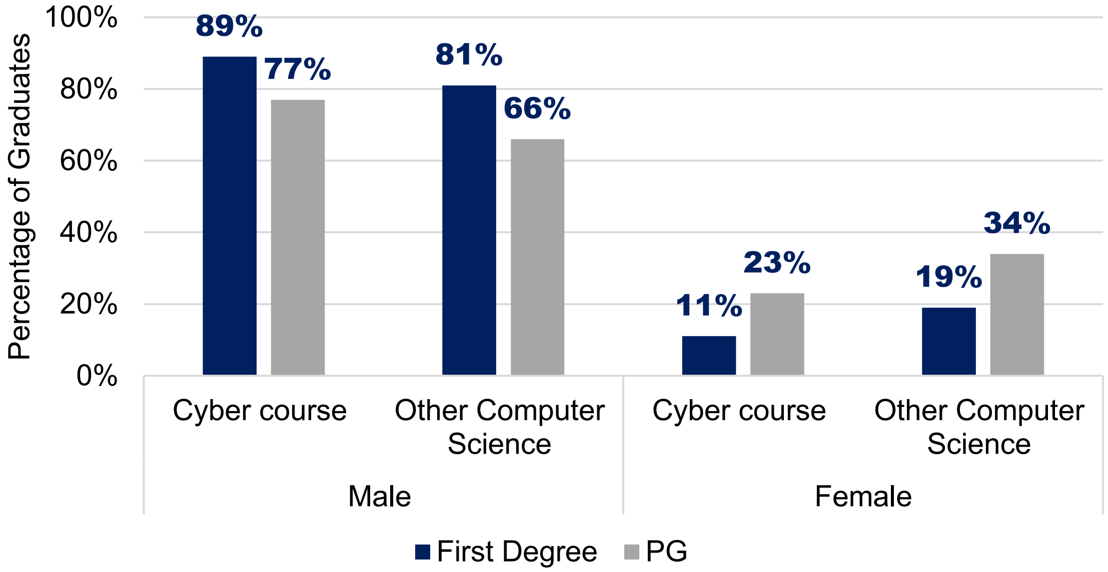
Student profiles

This section provides the breakdown of graduates in cyber security and computer science courses for the latest year of available data (2020/21), in terms of gender identity, ethnicity, domicile, age and entry from state schools.

Gender Identity

In previous research, there has been a significant gender gap identified within the cyber security industry. Figure 8.1 highlights the gender split at undergraduate and postgraduate level for both cyber security courses and other computer science courses. This highlights that within cyber courses only 11% of graduates at undergraduate level and 23% at postgraduate level identify as female. This suggests a small increase in postgraduate participation from female students since the previous year (17% in 2019/20); however, the participation levels remain low compared to both computer science, and wider HE participation.

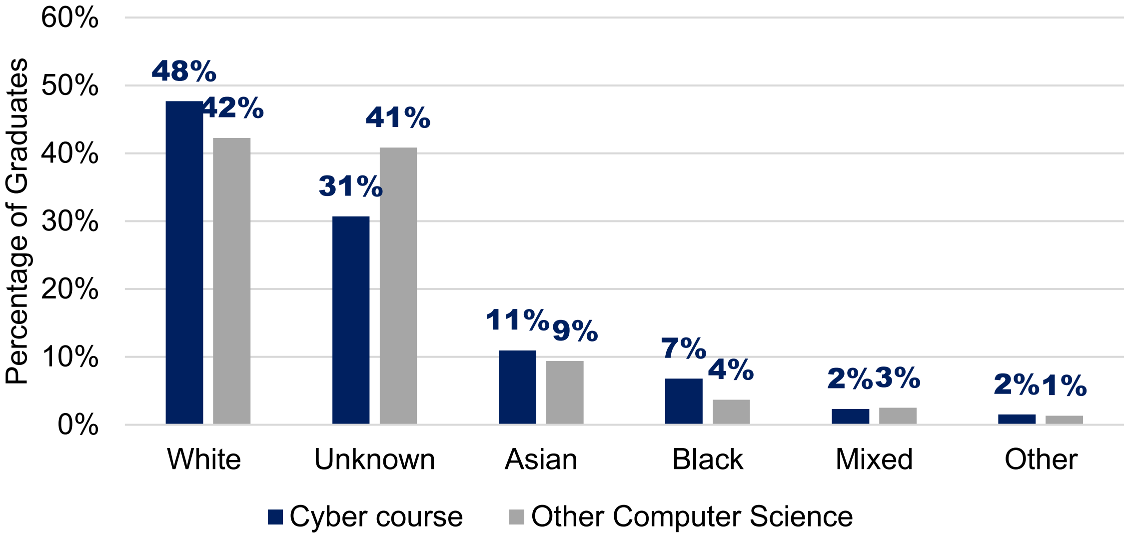
Figure 8.1: Gender Identity of Cyber Security and Computer Science Graduates (2020/21)



Source: Analysis of Jisc / HESA data (2020/21).
Base: Cyber courses, n =4,350 & Computer Science, n =39,050

Figure 8.2 highlights that in the academic year 2020/21, at least 22% of cyber security and 17% of computer science students were from ethnic minority backgrounds. There is a small decrease in the proportion of ethnic minority students, with a 2% decrease for cyber security students and a 2% decrease for computer science students from the figures set out in section 10.1 of the Cyber Security Skills in the UK Labour Market Report (2022), albeit this may also be due to the rise in the proportion with unknown ethnicity.

Figure 8.2: Ethnicity of Cyber Security and Computer Science Graduates (2020/21)

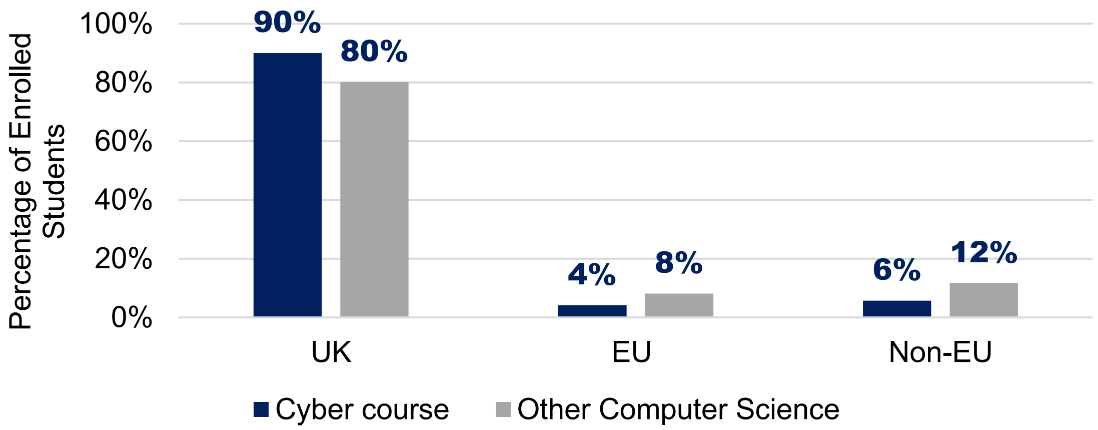


Source: Analysis of Jisc / HESA data (2019-2021).
Base: Number of students with ethnicity provided: Cyber courses, n =3,925 & Computer Science, n =32,094

Domicile

The following figures explore the domicile (i.e. prior home addresses) of cyber security and computer science students in 2020/21. Figure 8.3 shows that 90% of cyber undergraduate students are from the UK. When compared with figures from the Cyber Recruitment Pool research (2018/19), the ratio of students from the UK (c.90%) has remained relatively consistent. A closer look at cyber security students at all levels (undergraduate and postgraduate) in 2020/21 shows that 77% of students were from the UK, 18% of students were non-EU, and 4% were from the EU.

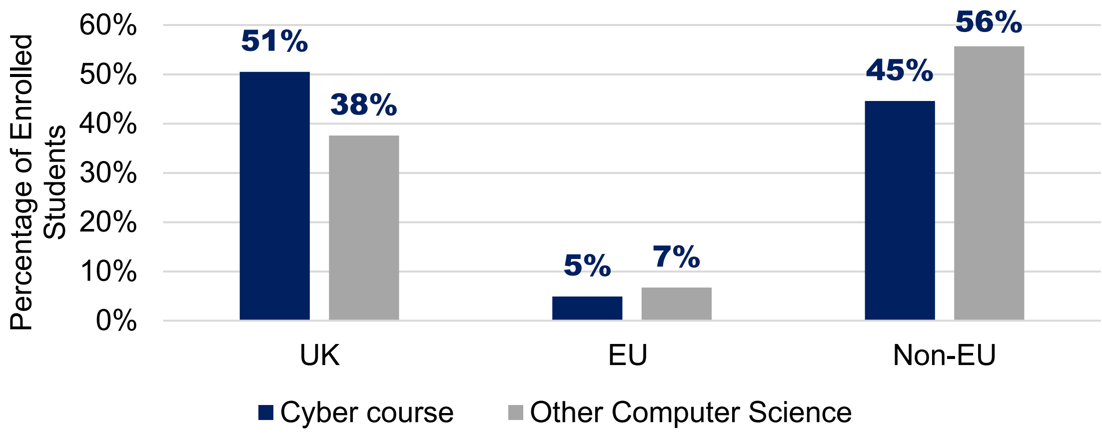
Figure 8.3: Domicile of Undergraduate Cyber Security and Computer Science Enrolled Students (2020/21)



Source: Analysis of Jisc / HESA data (2020/21).
Base: Cyber courses, n =12,990 & Computer Science, n =106,820

Figure 8.4 highlights that the proportion of non-EU computer science postgraduate students has increased from 43% in 2019/20 to 56% in 2020/21, surpassing enrolment levels of UK students. This highlights the international attractiveness of the UK as a destination for computer science higher education courses; however, there may be a need to focus on ensuring this translates to an increase in talent supply for the UK.

Figure 8.4: Domicile of Postgraduate Cyber Security and Computer Science Enrolled Students (2020/21)



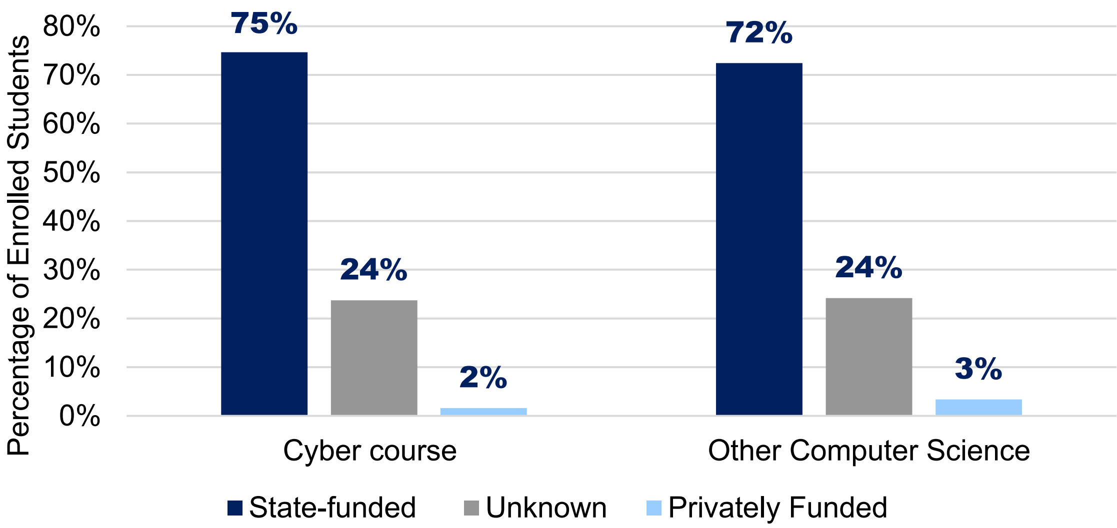
Source: Analysis of Jisc / HESA data (2020/21).
Base: Cyber courses, n =6,210 & Computer Science, n =52,310

Further analysis shows that of the 1,068 cyber security graduates from the UK who were employed (and provided job role SOC2020 code) at the time of the Graduate Outcomes survey, 90% (964) reported that they stayed in the UK to work. This suggests that there is strong domestic graduate retention in the UK cyber security market.

State School Marker

The marker for 'state school' attendance is a useful proxy for exploring the diversity of students entering particular courses. Figure 8.5 sets out the proportion of UK domiciled students enrolled in cyber security and other computing courses. This highlights that at least 75% of students enrolled in cyber security courses are from state school backgrounds, compared to 72% for wider computer science courses. A very small proportion are from privately funded schools. Please note that there is also a significant group of 'unknown'; many of these students are likely to have attended state-funded schools also.

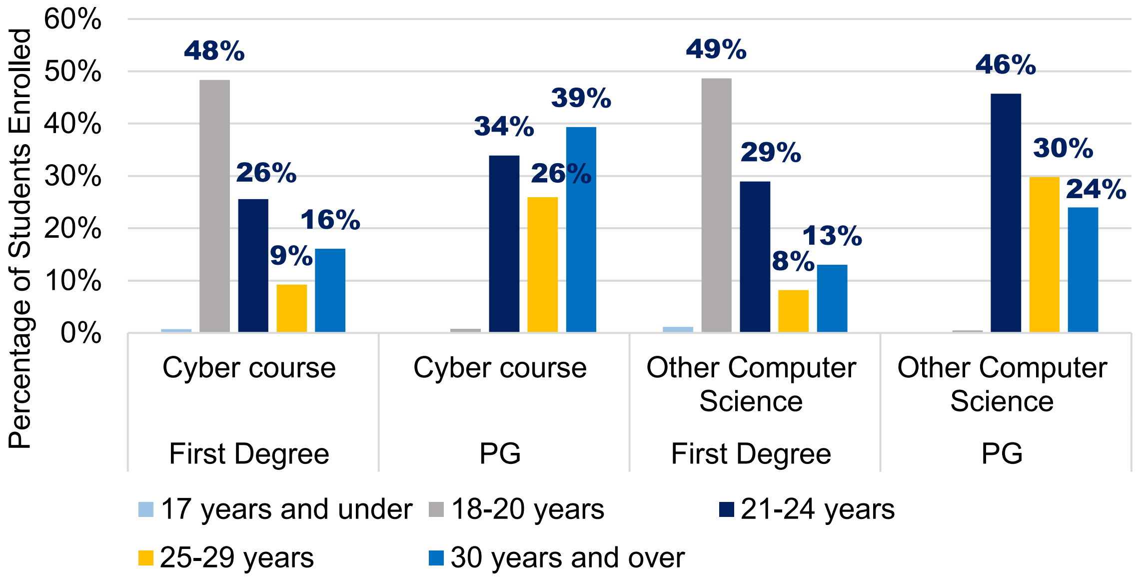
Figure 8.5: State School Marker – Cyber Security and Computer Science students from the UK – Enrolled in 2020/21



Source: Analysis of Jisc / HESA data (2020/21).
Base: UK Domiciled students enrolled in Cyber courses, n =14,840 & Computer Science, n =105,290

At undergraduate level, Figure 8.6 highlights that the 74% of students enrolled on cyber security courses are within the 18 to 24-year age range. However, 25% per of undergraduate students enrolled in cyber security courses are 25 or over, and this figure increases to 65% at post-graduate level. This may indicate significant demand among older students or those seeking to upskill in cyber security to do so through the higher education system.

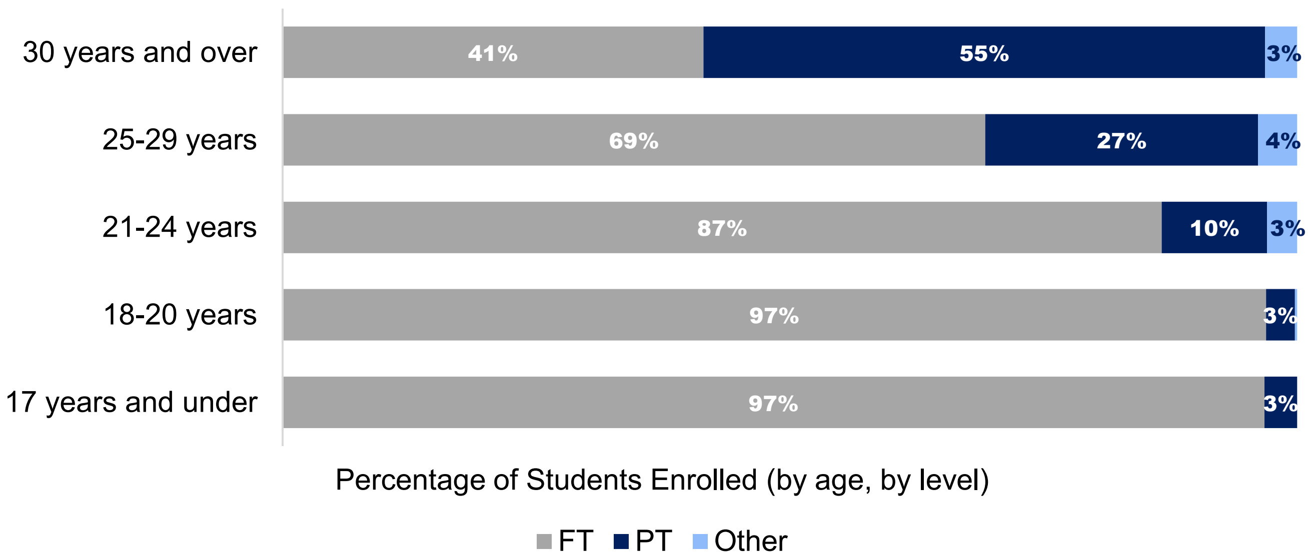
Figure 8.6: Age of Cyber Security and Computer Science Students – Enrolled in 2020/21



Source: Analysis of Jisc / HESA data (2020/21).
Base: Cyber courses, n =19,200 & Computer Science, n =159,130

Figure 8.7 sets out the percentage of students enrolled in full-time, part-time, and other forms of study by age. This highlights that younger students are more inclined to study full-time, whilst more mature students are likely to study part-time, typically given work or other commitments. This means that exploring sufficient provision of part-time or distance learning opportunities in cyber security for mature students may help to stimulate increased demand.

Figure 8.7: Age of Cyber Security Students – Enrolled in 2020/21 (all levels)



Source: Analysis of Jisc / HESA data (2020/21).

Base: Full-time, n =14,760; Part-time, n =4,010 & Other, n=430[17]

Graduate Outcomes

The most recent HESA data on graduate outcomes covers the 2019/20 academic year, based upon the responses to the Graduate Outcomes Survey.

Graduates are asked about their activities within approximately 15 months after they complete their studies, so the responses received can show activity taking place between December 2020 and September 2021 (for those that completed the Graduate Outcome Survey following their studies). Of the 3,670 students that graduated in cyber security courses in 2019/20, just over 50% (1,850) participated in the Graduate Outcomes Survey. Similarly, just over 50% (16,750) of the computer science graduates participated in the Graduate Outcomes Survey.

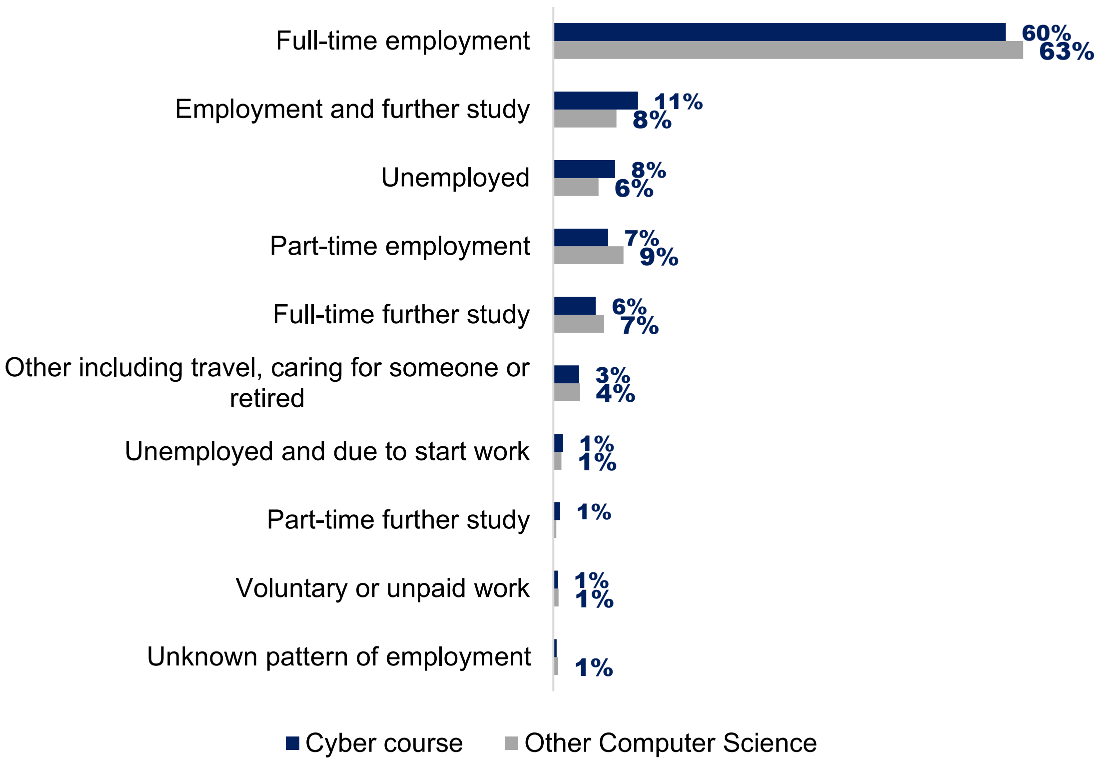
Figure 8.8 shows the overall graduate outcomes for those that graduated in the academic year 2019/20. The results show that in the most recent year, 60% of cyber security graduates entered full-time employment, and a further 11% of cyber security graduates entering employment and further study. This is slightly lower than the levels seen in the previous year (62% and 12% respectively). A further 7% entered part-time employment.

This means that, of the c.3,700 students that graduated in cyber security in 2019/20, and for the 4,360 cyber security graduates in 2020/21, we estimate that approximately 80% of these will enter the labour market within 15 months. We explore sectors and roles for these graduates in subsequent subsections.

We also note that 8% of cyber security graduates were unemployed within fifteen months of graduating. This compares to 6% across all graduates[18], potentially indicating a challenge with respect to ensuring that cyber security graduates have the soft skills and interview skills, as well as ability to pass technical tests often required to secure a graduate role.

[17] Percentages less than 1% are not labelled, i.e. 0.22% of 18–20-year-olds reported other.
[18] https://www.hesa.ac.uk/news/16-06-2022/graduate-outcomes-data-statistics-201920

Figure 8.8: Overall Graduate Outcomes (2019/20 academic year)



Source: Analysis of Jisc / HESA data (2019/20).
Base: Cyber courses, n = 1,850 & Computer Science, n =16,750

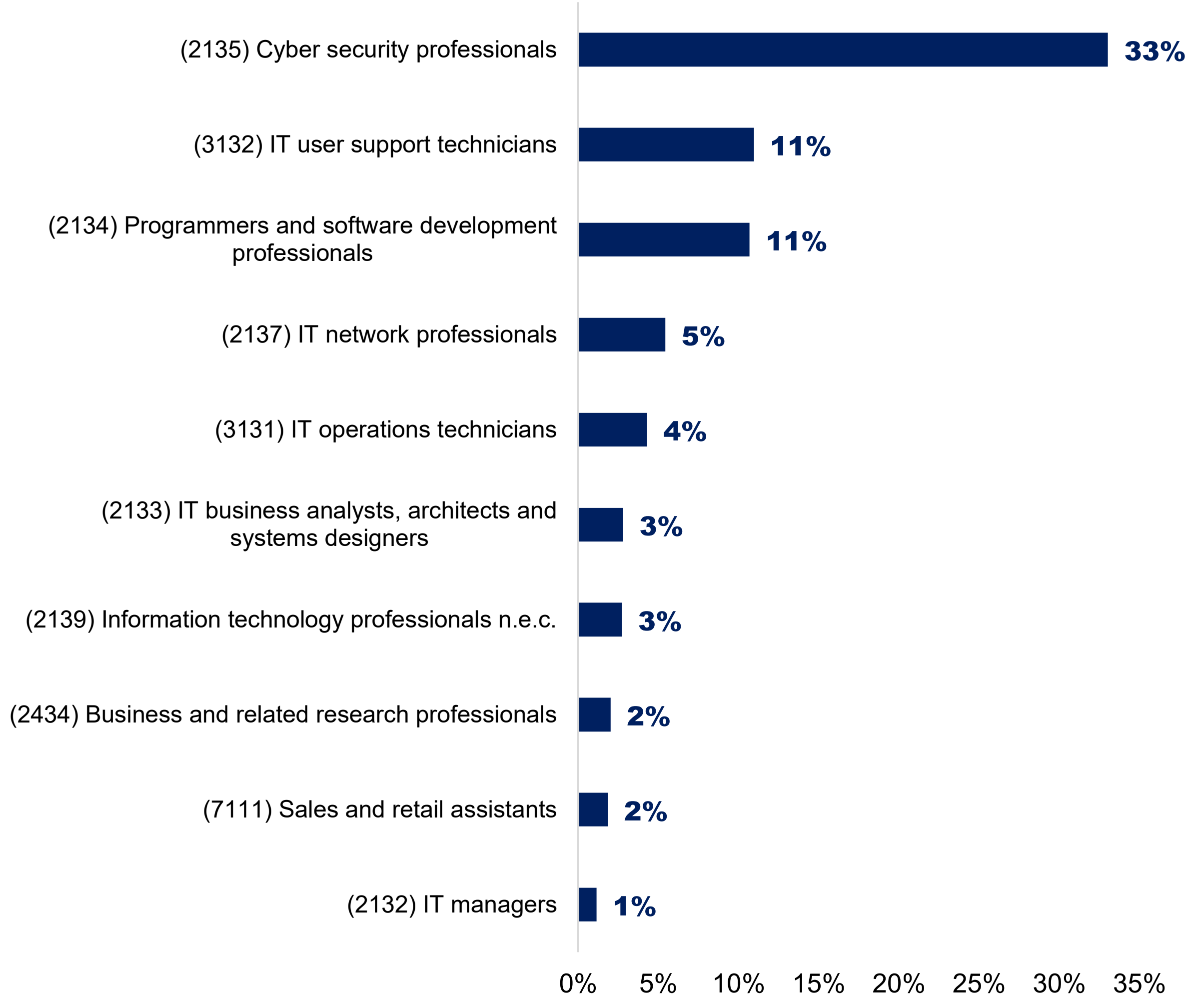
Employment outcomes

Using the Standard Occupational Classification (SOC) codes for the 2019/20 academic year, we can understand the most popular careers for cyber security graduates. Figure 8.9 displays the top job roles, based on the proportion of cyber graduates in each role.

The data highlights that 33% of cyber graduates are employed in cyber security professional roles; this has remained relatively consistent from the 2018/19 academic year and may demonstrate continued use of the new SOC code for ‘cyber security professionals’, as well as more focused employment outcomes.

The proportion of cyber graduates in programming and software development professional roles has also remained steady at 11% in 2018/19 and in 2019/20. However, a substantial proportion of cyber graduates move into IT-related roles that may require an element of cyber specific knowledge, and many of those that state they are in ‘programming roles’ etc may ultimately work for cyber security employers.

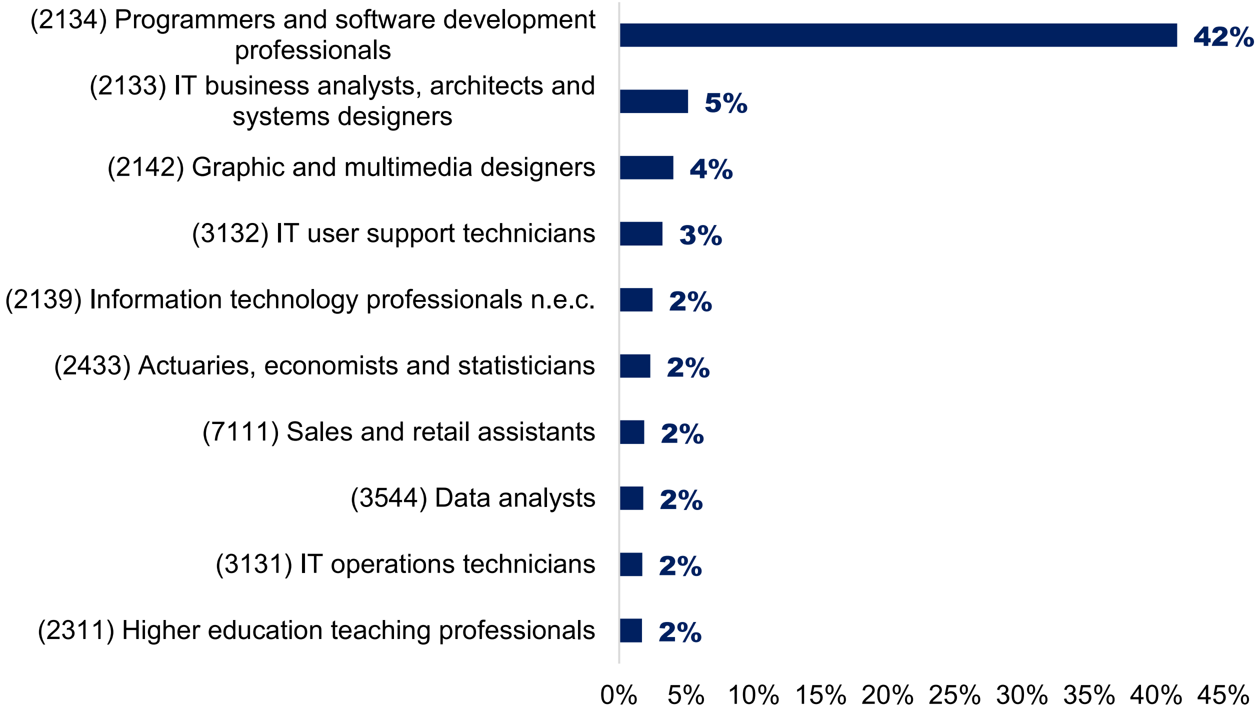
Figure 8.9: Top job roles based on Standard Occupational Classification (SOC) 2020 for cyber security graduates (2019/20)



Source: Analysis of Jisc / HESA data (2019/20).
Base: Total Graduates, n=1,340 in FT or PT employment

Figure 8.10 displays the top roles for computer science graduates, with over 40% of these graduates employed as programmers and software development professionals. The proportion of graduates in this role has decreased slightly from 46% in 2018/19 to 42% in 2019/20. However, only 1% of computer science graduates from 2019/20 consider that they are employed in cyber security professional roles (not shown on chart below). While this reflects an important inflow, it does highlight the race for talent across a wide range of digital sectors for computer science graduates.

Figure 8.10: Top job roles based on Standard Occupational Classification (SOC) 2020 for computer science graduates (2019/20)



Source: Analysis of Jisc / HESA data (2019/20).
Base: Total Graduates, n=12,240 in FT or PT employment

With respect to the cyber recruitment pool, using the Graduate Outcomes Survey estimates, we assume that the following number of Higher Education graduates may be likely to enter IT and cyber security roles each year (Tables 8.4 and 8.5 below)

Table 8.4: Estimated number of graduates moving into IT-related roles

Course Type	Number of Graduates	Proportion in FT employment	Proportion in IT related roles	Implied Population
Cyber security	4,360	60%	95%	2,500 (rounded)
Other computer science	39,110	63%	85%	21,000 (rounded)
Total				23,500

Table 8.5: Estimated number of graduates moving into cyber security professional roles (SOC 2135)

Course Type	Number of Graduates	Proportion in FT employment	Proportion in SOC 2135 (cyber)	Implied Population

Cyber security	4,360	60%	33%	900 (rounded)
Other computer science	39,110	63%	c. 1%	250 (rounded)
Total				1,150

This data suggests that the volume of graduates moving into IT roles has increased by c.5,000 (+28%) since last year's report, and the volume of graduates in 'SOC2135 Cyber Security Professional' roles has remained similar to last year (1,150 compared to 1,200).

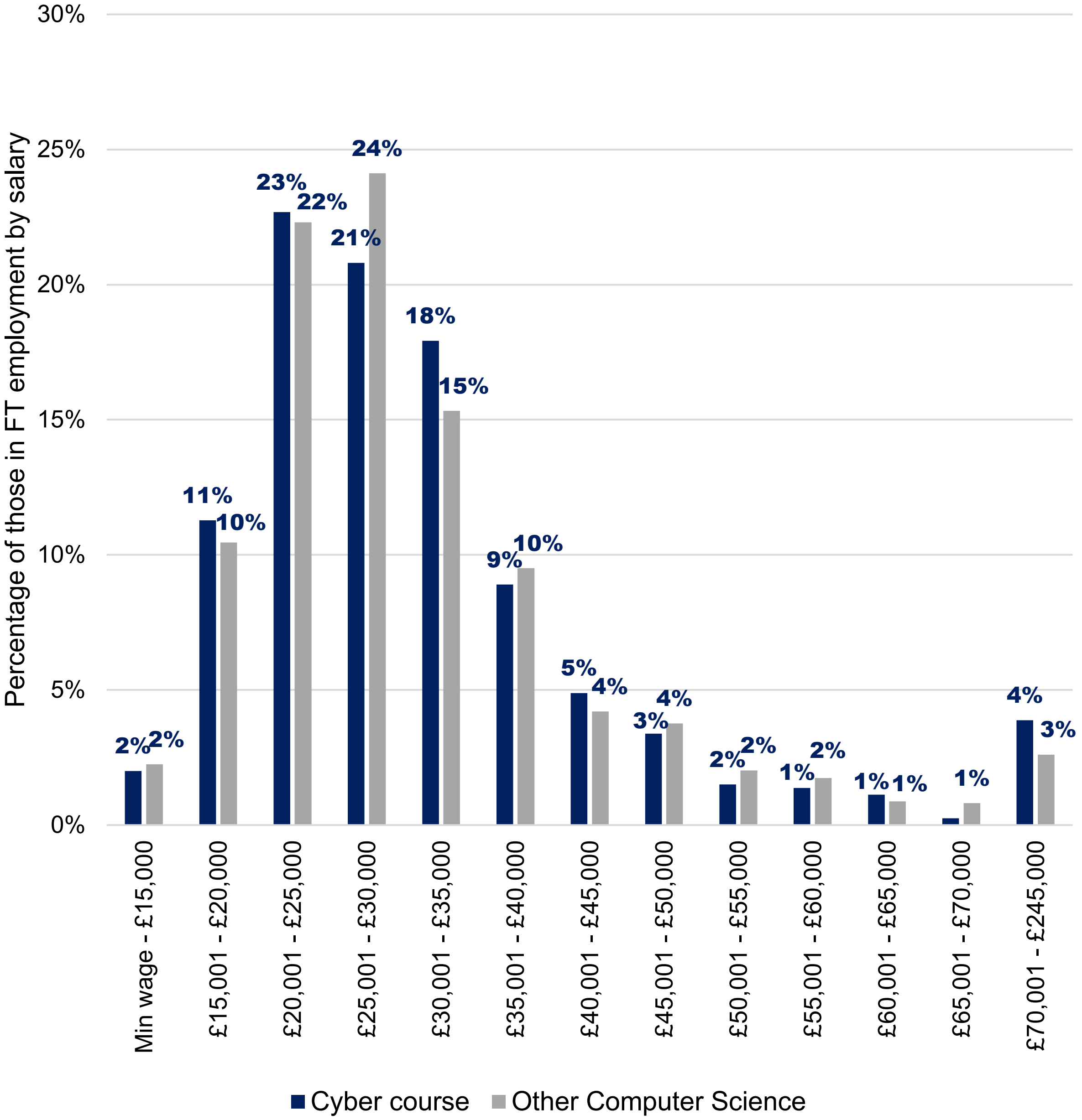
The previous report estimated that up to 4,000 graduates were likely to enter the broader cyber security labour market each year. This is because the SOC 2135 code is likely to significantly underestimate the volume of cyber security professionals (e.g. individuals working in cyber security related roles in programming, networks, consultancy etc). This means the response they provide for their current role in the Graduate Outcomes Survey may be coded into another area (such as programming or consultancy) even if their role is cyber security focused.

We note the increase in the number of IT and cyber security graduates, however, **we estimate a similar figure (c.4,000 graduates from the Higher Education sector may enter the broader cyber security labour market each year) as last year's estimate.**

Salaries

Analysis of Graduate Outcomes data also indicates salary bands for those in full-time employment. Figure 8.11 suggests that cyber security and computer science graduates have similar earnings, with median earnings in the £25,001 - £30,000 range in the 15 months after graduating.

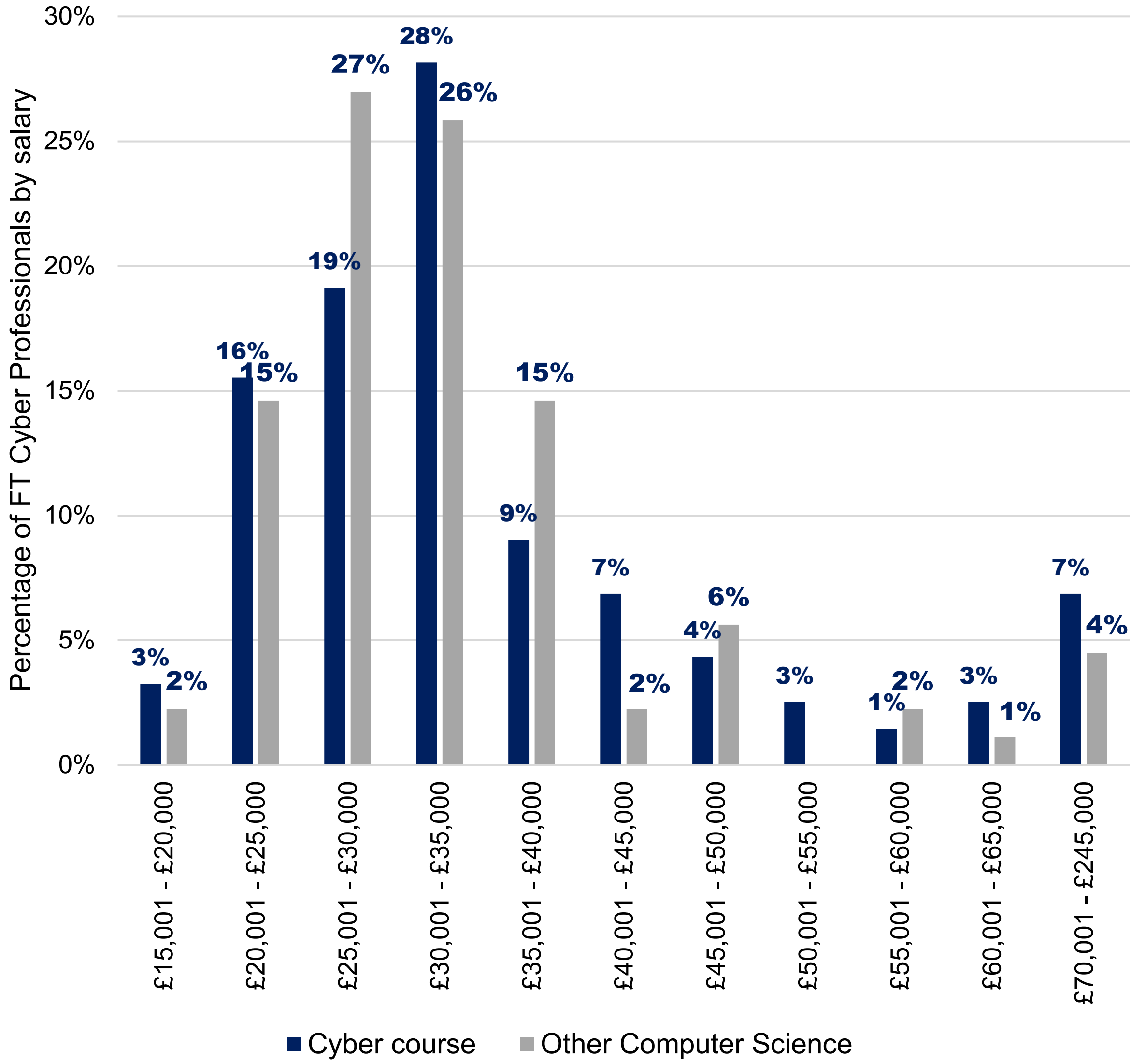
Figure 8.11: Reported Salaries by those in full-time equivalent employment (2019/20 academic year)



Source: Analysis of Jisc / HESA data (2019/20).
Base: Cyber courses, n =800 & Computer Science, n =7,280

Given the high proportion (43%) of graduates in cyber security professional roles, Figure 8.12 also explores the reported salaries for graduates in these roles. The median salary for cyber graduates in cyber professional roles is within the £30,000-£35,000 salary band, highlighting a wage premium at graduate level. Further, there are a higher proportion of graduates receiving higher salaries (e.g. over £70,000) when looking specifically at cyber professional roles.

Figure 8.12: Reported Salaries by those in full-time cyber professional roles (2019/20 academic year)



Source: Analysis of Jisc / HESA data (2019/20).
Base: Cyber courses, n =280 & Computer Science, n =90

Exploring all graduates within Cyber Security Roles in the UK

An additional bespoke data request was made for graduates from the academic years 2017/18, 2018/19, and 2019/20 who are employed in roles under the SOC213 (IT) code and SOC2135 (Cyber Security Professionals) across all degree pathways.

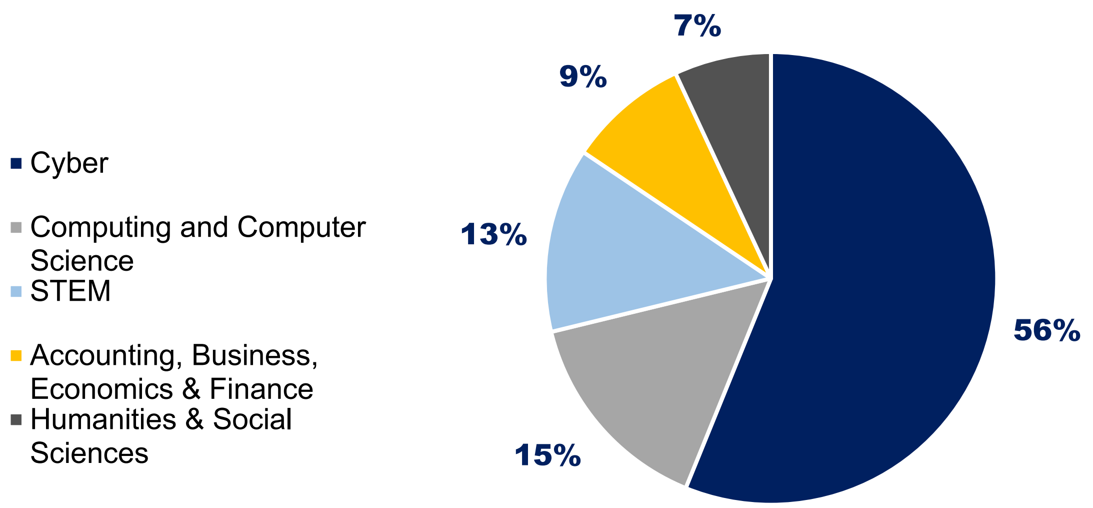
The purpose of this search is to identify graduates from any discipline (i.e. outside of cyber security or computer science courses) that are working in a cyber security role within fifteen months of graduating.

This data request covered a sample size of 764 graduates that completed the Graduate Outcomes Survey and identified their employment status under the SOC2135 code (cyber security professionals). This highlights that:

- 56% of these students studied a Cyber Security course;
- 15% studied Computing or Computer Science course;

- 13% studied a STEM related course (Science, Technology, Engineering and Maths);
- 9% studied Accounting, Business, Economics and/or Finance;
- 7% studied Humanities and/or Social Sciences.

Figure 8.13: Graduate course of Cyber Security Professionals (2019/20 academic year)



Source: Analysis of Jisc / HESA 2 data (2019/20).
Base: 764 Cyber Security Professionals; Cyber courses, n =430; Computer Science, n =120; STEM, n=100; Accounting, Business, Economics & Finance, n=70; Humanities & Social Sciences[19], n=50.

As such, Figure 8.13 suggests that although a substantial proportion of cyber security professionals come from cyber security, computing and computer science backgrounds, graduates from other disciplines are contributing to the cyber sector. This highlights the potential in encouraging graduates from a wide range of pathways into the cyber security profession, as well as post-graduate reskilling bootcamps.

8.2. The role of further education

As set out within the DCMS Cyber Recruitment Pool research, Further Education (FE) is an increasingly important route for students as they progress into industry or further study. Within the UK, many students who go on to study Cyber Security (or broader IT or computing courses) may undertake FE courses in IT, Computing, or Programming – which may include elements of cyber security within the syllabus. It is estimated that more than 50,000 students enrol each year on Level 3 class-based courses in the ICT subject area in England, of which approximately 60% study for a Diploma, c.25% for an A-Level qualification, and the remainder for Certificates or BTEC qualifications.

The subsequent sections explore the supply of talent into the cyber security labour market through routes such as apprenticeships, retraining and upskilling programmes, and wider inflows into the labour market (such as migration).

[19] Humanities and Social Sciences include (but are not limited to) courses such as history, philosophy and religion, political sciences, art, and modern languages.

Apprenticeships

Further Education (FE) continues to provide an increasingly important route for cyber security students, introducing them to the basics behind cyber security, networking, and IT. Further Education routes can provide a stepping stone towards a career in cyber security.

Table 8.6 sets out the number of apprenticeship enrolments, starts and achievements in ICT based apprenticeships in the academic years 2020/21 and 2021/22. [20]

The number of apprenticeship enrolments[21] in ICT subject areas in England has increased significantly in recent years, almost doubling from 21,110 in 2018/19[22] to 42,150 in 2020/21 and then by 9% from 2020/21 to 46,080 in 2021/22.

The number of apprenticeship starts[23] increased by 24% from 18,390 in 2020/21 to 22,820 in 2021/22, suggesting that there continues to be a strong increase in the number of students getting involved in ICT apprenticeships.

Table 8.6: Number of ICT apprenticeships (2020/21, 2021/22) in England

Apprenticeship Type	2020/21			2021/22		
	Enrolments	Starts	Achievements	Enrolments	Starts	Achievements
Intermediate Apprenticeship	3,450	40	2,550	560	70	420
Advanced Apprenticeship	18,540	9,180	5,220	22,110	12,310	4,310
Higher Apprenticeship	20,160	9,170	3,220	23,410	10,440	4,040
Total	42,150	18,390	10,990	46,080	22,820	8,770

Source: Department for Education (Academic year 2021/22) Apprenticeships and traineeships data.[24]

Table 8.7: Number starts in ICT apprenticeships (2021/22) in England

Detailed Level	Framework/Standard	Female	Male	Total Starts
2	IT and Telecoms Professionals	0	60	60
2	IT User	0	0	0
3	Cyber Security Technician-ST0865	10	30	40
3	Data Technician-ST0795	1,320	1,560	2,880
3	Digital Marketer-ST0122	1,950	1,430	3,380

[20] In Tables 8.6, 8.7, 8.8 and Figure 8.14, numbers have been rounded to the nearest ten due to statistical disclosure control.
[21] Apprenticeship enrolments are the count of enrolments at programme level for each academic year – learners will be counted for each apprenticeship they take and therefore, learners may be counted more than once.
[22] Ipsos MORI (2021) Understanding the Cyber Security Recruitment Pool. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973914/Ipsos_MORI_Cyber_Recruitment_Report_v1.pdf
[23] Apprenticeship starts are the count of apprenticeship programmes that begin in an academic year, showing the take-up of programmes – it is important to note that an apprentice is counted for each apprenticeship they start at a provider. Therefore, there could be some duplication.

3	Digital Support Technician-ST0120	120	330	450
3	Information Communications Technician-ST0973	360	3,460	3,820
3	Infrastructure Technician-ST0125	10	60	70
3	IT and Telecoms Professionals	10	130	140
3	IT Solutions Technician-ST0505	40	330	370
3	IT Technical Salesperson-ST0115	190	390	580
3	IT User	0	20	20
3	Radio Network Technician-ST0757	10	60	70
3	Software Development Technician-ST0128	80	390	470
3	Unified Communications Technician-ST0130	0	30	30
4	Applications Support Lead-ST0949	0	0	0
4	Business Analyst-ST0117	390	410	800
4	Cyber Intrusion Analyst-ST0114	0	0	0
4	Cyber Security Technologist (2021)-ST1021	60	270	330
4	Cyber Security Technologist-ST0124	10	20	30
4	Data Analyst-ST0118	1,550	2,460	4,010
4	DevOps Engineer-ST0825	70	260	330
4	IT and Telecoms Professionals	0	0	0
4	Junior Animator-ST0488	0	10	10
4	Network Engineer-ST0127	50	860	910
4	Software Developer-ST0116	250	790	1,040
4	Software Tester-ST0129	40	90	130
4	Unified Communications Trouble Shooter-ST0131	0	0	0
6	Cyber Security Technical Professional (Integrated Degree)-ST0409	20	90	110
6	Data Scientist (Integrated Degree)-ST0585	70	170	240
6	Digital and Technology Solutions Professional (Integrated Degree)-ST0119	440	1,140	1,580
6	Digital User Experience (UX) Professional (Integrated Degree)-ST0470	40	40	80
7	Artificial Intelligence (AI) Data Specialist-ST0763	70	170	240
7	Digital and Technology Solutions Specialist (Integrated Degree)-ST0482	160	460	620
7	Game Programmer-ST0953	10	10	20
	Total	**7,330**	**15,530**	**22,860**

Source: Department for Education (Academic year 2021/22) Apprenticeships and traineeships data.

Role of Apprenticeships / Degree Apprenticeships

Table 8.8 sets out the number apprenticeship enrolments, starts and achievements[25] in England. This suggests that the number of apprentices has increased in the last three years, a further increase from the previous findings in 2018/19 (c. 600 enrolments).

Table 8.8: Number of apprenticeship enrolments, starts and achievements in England, 2019 to 2022

Framework/Standard	Type	2019/20	2020/21	2021/22
Cyber Intrusion Analyst-ST0114	Enrolments	30	20	10
Cyber Security Technical Professional (Integrated Degree)-ST0409	Enrolments	80	170	220
Cyber Security Technician-ST0865	Enrolments	0	20	60
Cyber Security Technologist (2021)-ST1021	Enrolments	0	20	340
Cyber Security Technologist-ST0124	Enrolments	660	680	380
Total	**Enrolments**	**770**	**910**	**1,010**
Cyber Intrusion Analyst-ST0114	Starts	10	0	0
Cyber Security Technical Professional (Integrated Degree)-ST0409	Starts	50	70	100
Cyber Security Technician-ST0865	Starts	0	20	40
Cyber Security Technologist (2021)-ST1021	Starts	0	20	320
Cyber Security Technologist-ST0124	Starts	250	270	30
Total	**Starts**	**310**	**380**	**490**
Cyber Intrusion Analyst-ST0114	Achievements	10	10	0
Cyber Security Technical Professional (Integrated Degree)-ST0409	Achievements	0	0	30
Cyber Security Technician-ST0865	Achievements	0	0	0
Cyber Security Technologist (2021)-ST1021	Achievements	0	0	0
Cyber Security Technologist-ST0124	Achievements	50	140	140
Total	**Achievements**	**60**	**150**	**170**

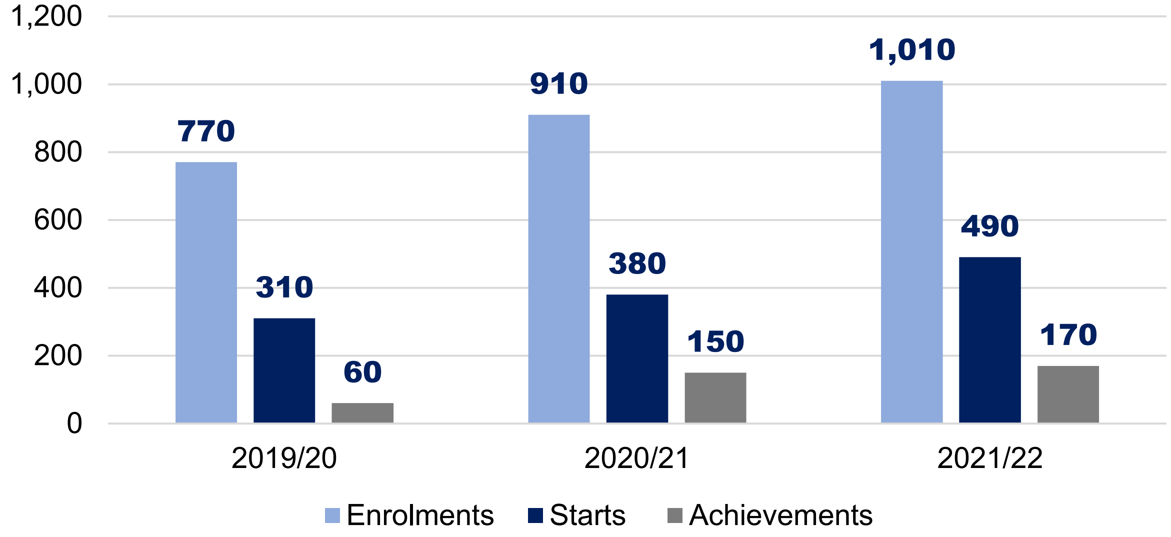
Source: Department for Education (Academic year 2021/22) Apprenticeships and traineeships data.

[25] Apprenticeship achievements signify a learner reaching the end point of assessment; this is not necessarily the same as the end of their learning/apprenticeship.

The increase in the number of students starting, enrolled in, and achieving qualifications in cyber security focused apprenticeships is highlighted further by Figure 8.14. This emphasises the steady increase in cyber security apprentices over time.

This data highlights that there are 490 new starts into the cyber recruitment pool in England in 2021/22, and this figure will be higher for across the United Kingdom.

Figure 8.14: Number of apprenticeship enrolments, starts and achievements in England, 2019 to 2022



Source: Department of Education
Base: 4,250 students who have started, been enrolled in or achieved apprenticeships in England, 2019-2022: 2019/20, n=1,140; 2020/21, n=1,440; 2021/22, n=1,670.

Retraining and Upskilling

In addition to qualifications obtained through further and higher education, several employers will also look for potential employees with relevant skills often affirmed through certification and training providers. In recent years, there has been increased emphasis on how certifications and training models can rapidly upskill people to move into or increase knowledge of cyber security roles.

Further, the provision of innovative training models such as cyber security academies and bootcamps, and enhanced access to low-cost online training platforms has also driven enhanced interest in cyber security training.

As mentioned previously, within the business survey of 180 cyber sector firms, among qualified staff:

- 45% of staff held a specialist higher education qualification (e.g. a degree) related to cyber security
- 38% of staff held a general computer science / IT degree;
- 29% of firms had staff that held a cyber security apprenticeship
- 15% were qualified through another apprenticeship role;
- 74% of staff held some form of other technical accreditation.

This highlights the importance of a wide range of technical accreditation and apprenticeships, in addition to higher education. The Cyber Recruitment Pool (2021) research explores these routes in depth. The following section sets out updated estimates and commentary where available.

- **Certifications**: Further, within the UK, as of January 2023, there are approximately 8,500 (ISC)² members in the UK holding the CISSP certification (an increase of 8% since January 2021. CompTIA is also a prevalent certification provider, offering Network+, CySA+, Security+, PenTest+ and more. In 2019, CompTIA announced that over 500,000 individuals had earned the CompTIA Security+ certification globally.
- **Retraining and Upskilling Initiatives:** The UK is home to a range of retraining and upskilling initiatives. This includes providers such as Immersive Labs, Capslock, QA, SANS and more, as well as online provision. Last year's report noted that there is limited data available on the quantification of these routes; however, it is possible that up to 1,500 individuals may currently enter the recruitment pool through this route. This is based upon knowledge of a number of initiatives identified across the UK e.g. Assured Skills Academies, funded skills initiatives, Career Transition Partnership etc. It is likely that this figure has increased in the last twelve months.
- **Armed Forces:** Over 14,000 individuals leave the Armed Forces each year. In 2020/21, almost 9,500 service leavers used support from the Career Transition Partnership (a scheme to support leavers into employment). Of these, 473 entered Science, Research, Engineering and Technology Professional roles in 2020/21, of which 56 reported a role as a 'Cyber Security Professional' under SOC2020.
- **Attracting international talent:** In addition to upskilling the population, the cyber security recruitment pool can also be increased through exploring the UK's capacity to attract international talent, and encourage global knowledge transfer. The Global Talent Visa programme has approved c.2,300 visas (between Jan 2020 – August 2021), and includes researchers and employees coming to the UK to engage in cyber security activity. However, we do not have a granular breakdown of these figures.
- **DfE Bootcamps:** The Department for Education offers Skills Bootcamps, with flexible courses available for up to 16 weeks. The Bootcamps provide a range of cyber-related courses, including cloud engineering, computer science, cyber security, and cyber technician skills. On completion of the course, participants are offered a job interview with an employer.

Last year's report estimated these could be generating in the region of c. 2,500 individuals into the cyber recruitment pool each year. We retain this estimate as a conservative figure. In summary, we estimate that the UK inflows into the cyber security recruitment pool have remained relatively consistent within the last twelve months, with 7,000 entrants consisting of:

- Approximately 4,000 graduates from cyber security, computer science, or other HE courses
- Approximately 2,500 individuals through retraining, reskilling, career conversion, or international migration
- At least 500 new apprenticeship starts (in England).

8.3. Estimating the size of the cyber security recruitment pool

The previous Cyber Skills in the UK Labour Market (2022) research drew an estimate of c.131,000 cyber security professionals working in the UK. This section revisits and updates the previous estimate, using updated data from the last 12 months. In order to create this estimate, we have reviewed various data sources, covered in this section.

We estimate that the current cyber security workforce has risen slightly to c.133,400 FTEs in 2022.

DSIT Cyber Security Sectoral Analysis (2023) workforce estimate

Since 2017, DSIT has tracked the size and scale of the UK's cyber security sector within the Cyber Sectoral Analysis. Whilst this only covers full-time equivalent (FTE) employment related to cyber security roles, it provides a useful indicator of the scale of the number of jobs within private sector firms that trade in cyber security products and services. The relevant figures from all published sectoral analyses to date are shown in Table 8.9.

In the most recent year, employment in the cyber security sector has grown by 10%, and the sector has experienced double-digit growth in previous years (outside 2020).

Table 8.9: Number of FTEs in the UK Cyber Security Sector, 2017 to 2022

Year	Number	Increase	Annual Growth
2017	31,339		
2018	36,000 (estimated as no study commissioned in 2018)	4,661	15%
2019	42,855	6,885	19%
2020	46,683	3,828	9%
2021	52,727	6,044	13%
2022	58,005	5,278	10%

ISC2 Cybersecurity Workforce Study

The 2022 ISC2 Cybersecurity Workforce Study suggests there are c.339,000 (+13% from 2021) individuals in the UK cyber security workforce, with a shortage of c.57,000.

It is not possible for us to validate their estimate with our data, given the differences in methodologies between our two studies (outlined later in this section) and limited published technical information on the UK sample size and representativeness of the ISC2 data. The estimate may also be likely to have a margin of error around it.

Cyber Security Workforce Estimates

The ONS recently updated the Standard Occupation Classification system to 'SOC2020', which includes job classifications for 'Cyber Security Professionals'. This will be beneficial in future years to support estimations of the number of people working in the UK as 'cyber security professionals', with potential to explore this data in recoded iterations of the Labour Force Survey and Annual Population Survey (expected from summer 2023).

However, this means that this study estimates the size of the UK's cyber security workforce using other variables, including use of the DSIT Cyber Security Sectoral Analysis research, job vacancy analysis, and wider modelling.

Our estimates suggest that:

- There are at least 122,000 individuals in these roles based upon industry growth rates.
- The previous Cyber Skills in the UK Labour Market report estimated a mid-point of c.131,000 individuals in the cyber security workforce.
- The previous study also estimated that c.7,000 individuals would enter the cyber security workforce in 2022, and a further 4,600 would leave the workforce, implying a net increase of c.2,400.
- **As a conservative estimate, we estimate there are c. 133,400 in the cyber security workforce as of end of 2022.**

Future annual estimates should explore enhanced use of LFS and APS data using SOC2022 (2135) Cyber Security Professionals to further test and refine these estimates.

8.4. Estimating the Cyber Workforce Gap

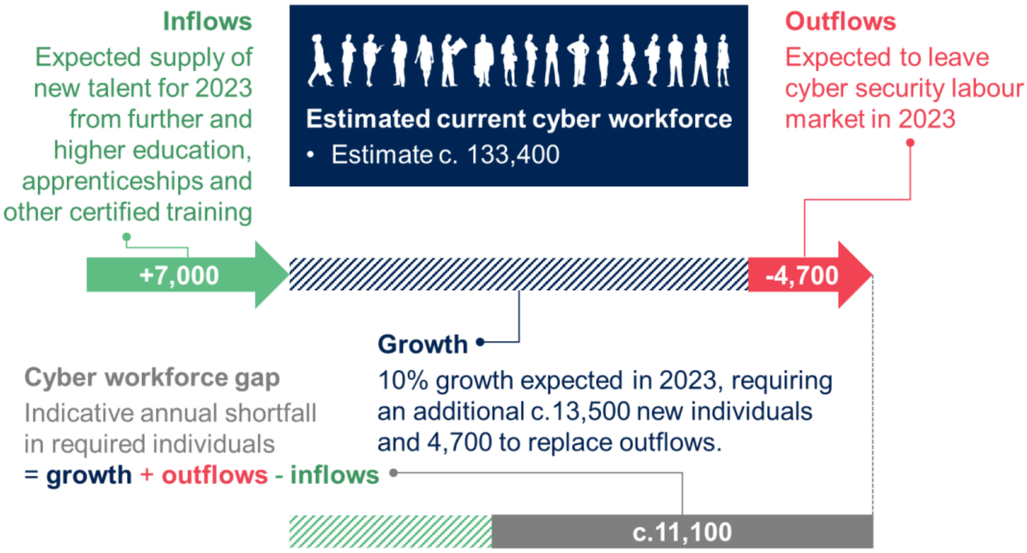
The previous cyber recruitment pool research indicated a shortfall of c.14,100 individuals per year in the cyber security workforce – the cyber workforce gap. To note, this is different to the skills gaps and skills shortages discussed in Chapters 4 and 6.

This year, we revise this estimate based on the latest data to 11,200 individuals a year (a decrease of 2,500). The constituent parts of this calculation are as follows, bringing together the estimates from the rest of this chapter:

- For 2022, we estimate the current workforce to be in the region of 133,400 individuals
- A total of c.7,000 individuals entered the cyber security workforce in 2022. This encompasses the c.4,000 entering from Higher Education (section 10.1), up to 2,500 undertaking career conversion, retraining, or entering the UK pool elsewhere, and up to 500 involved in apprenticeships in cyber security
- As Chapter 8 shows, up to 3.5% of cyber security employees leave the sector in a given year. This provides an estimate of c.4,700 leavers each year
- Employment in the cyber security sector has increased by 10% within the last year according to the DCMS Cyber Sectoral Analysis 2022. This suggests a need for c.13,500 new people each year to meet demand, in addition to the c.4,700 to replace those exiting the sector, i.e. a total requirement of c. 18,200 per year
- Taken together, these findings suggest a net annual shortfall of c.11,200 people in 2022. This is a decrease of c.2,500 from the 2021 estimate; however, this figure is smaller due to a smaller growth rate in the size of the current workforce (from 13% to 10%). The gap remains persistent, and annually cumulative in effect.

Figure 8.15 concludes with a visual summary of this workforce gap for 2022.

Figure 8.15: Summary Diagram of the 'Cyber Workforce Gap



Outsourcing cyber security

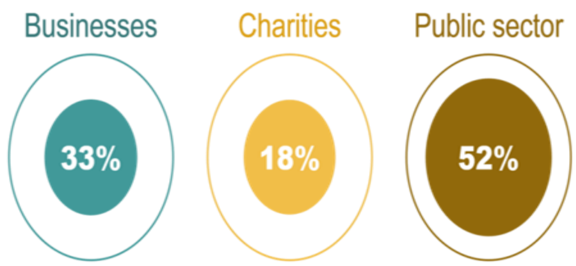
This brief chapter looks at the organisations (outside the cyber sector) that outsource any aspects of their cyber security and outlines what they outsource.

- Around 1 in 3 businesses (33%) outsource any aspects of cyber security, which is consistent with the previous year (when it was 32%). Outsourcing cyber security remains much more common in the public sector (at 52%), in particular in comparison with charities (18%).
- Setting up firewalls, detecting and removing malware, and incident response or recovery are the 3 most commonly outsourced cyber security functions. Among the 33% of firms that outsource cyber security, 87% specifically outsource functions that require more advanced technical skills, such as interpreting malicious code.
- External Security Operations Centres (SOCs) are used by a small proportion of businesses overall (17%). They are more commonly used by large businesses (37%) and public sector organisations (28%).

9.1. The prevalence of outsourcing

18% of charities outsource any aspect of cyber security. In comparison, 33%of businesses outsource any aspects of cyber security (Figure 9.1), and the proportion is higher still among public sector organisations, where 52% outsource any aspects of their cyber security. This is consistent with 2022.

Figure 9.1: Percentage of organisations that outsource any aspects of their cyber security to external providers



Bases: 1006 businesses; 214 charities; 102 public sector organisations

Outsourcing of cyber security functions remains more prevalent in the finance and insurance sector (62% vs. 34% overall), which has been the pattern for the previous 3 years. Information and communication (21%) and food or hospitality businesses (23%) are among the least likely to outsource cyber security. Businesses in the South West are also less likely than average to outsource (27% vs. 34% overall), which is consistent with the previous year.

9.2. What aspects of cyber security do organisations outsource?

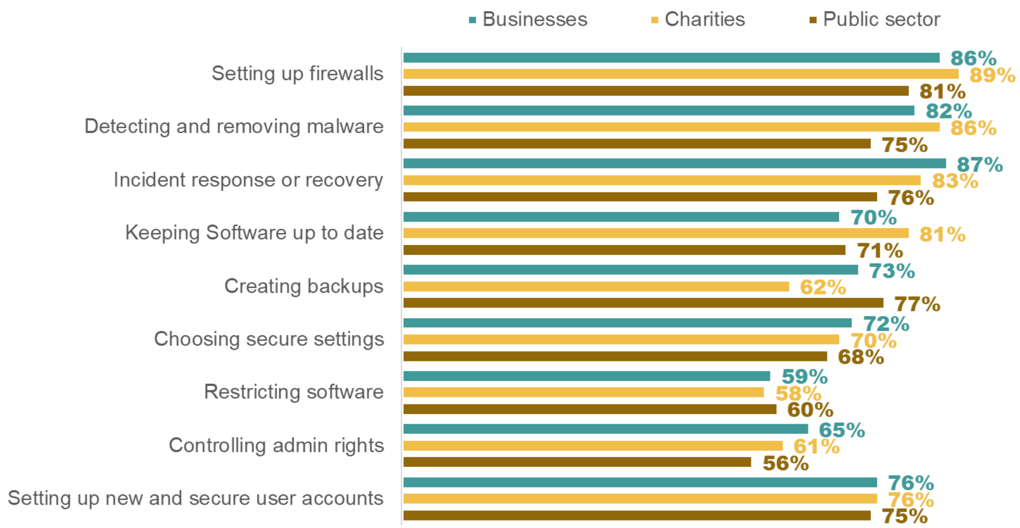
Outsourcing of basic functions (including incident response)

Figure 9.2 shows the kinds of basic functions (as opposed to the more advanced functions which are covered in the next sections) that get outsourced, among the organisations that outsource any aspects. Please note that the charities and public sector samples are relatively small for this question, so have wider margins of error than in the rest of the report.

For businesses, setting up firewalls, detecting and removing malware, and incident response or recovery remain the 3 most commonly outsourced functions in this list. Around 8 in 10 of those that outsource any aspects of cyber security have at least one of these functions incorporated into this service. At the other end, restricting software and controlling admin rights continue to be the 2 functions least likely to be outsourced. These results are consistent with last year's study.

Most organisations still expect to perform various aspects of cyber security in-house, even if they use external providers for some functions. Among those that outsource, a total of 32% of businesses, 25% of charities and 38% of public sector organisations pass responsibility for all the functions mentioned in Figure 9.2 to their external cyber security providers.

Figure 9.2: Percentage of organisations outsourcing various basic cyber security functions, among those that outsource any aspects



Bases (among those that outsource cyber security): 328 businesses; 38 charities*; 53 public sector organisations
*small base

Use of Security Operations Centres (SOCs)

The use of Security Operations Centres (SOCs) remains consistent with previous years. A total of 17% of businesses and 8% of charities use one. Large businesses (37%) and public sector organisations (28%) are more likely to use SOCs. These results are consistent with last year, when this question was first asked (when 16% of businesses said they used SOCs).

Outsourcing of other more advanced functions

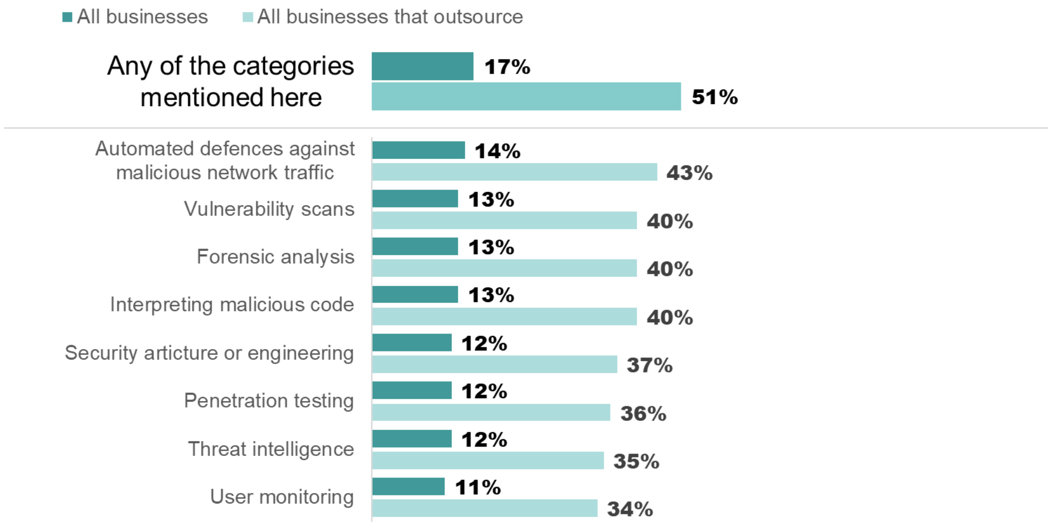
Figure 9.3 shows the other kinds of advanced functions that get outsourced. It shows two sets of figures – the proportion of the 33% of businesses that outsource any aspects of cyber security and the percentage of all businesses (i.e. including those who do and do not outsource).

In total, 17%) of businesses outsource any of these advanced cyber security functions. This proportion is markedly higher among large businesses (43%). There are too few public sector organisations and charities in our sample to analyse for this question.

The 8 categories of advanced functions reflect the split used across this study, in terms of basic versus advanced technical cyber security skills (which links back to the definition and categorisation of cyber security skills established in the 2021 study).

As in previous years, there is a broadly even spread in terms of 7 out of the 8 of these categories. However, this year, automated defences against malicious network traffic has been included in our classification of advanced cyber skills.

Figure 9.3: Percentage of businesses outsourcing various advanced cyber security functions, among those that outsource any aspects



Bases: 1,006 businesses; 328 businesses that outsource cyber security

In the qualitative research, we found that while some organisations were outsourcing all or most of their cyber security function, others were outsourcing only advanced functions. This was because they did not have the specialist skills or the ability to provide 24/7 cover. Outsourcing rather than building internal capability was regarded as a better use of their resources.

"It's all about economies of scale. A SOC [Security Operations Centre] team is made of people with all sorts of technical disciplines. It needs to be 24/7, they have to work nights. Building that yourself is going to be costly in any organisation. Managed service providers can provide a SOC team that looks after a number of clients."
(Public sector organisation, 1,000 or more employees)

Outsourcing more advanced functions was also used by organisations to mitigate against the risk of staff leaving.

"We often find it hard to hold on to staff who have that technical knowledge, but this is compensated by the fact that we outsource more cyber functions to a third party. So, this challenge is mitigated somewhat."
(Public sector organisation, 1,000 or more employees)

Conclusions

Our report shows the extent of the cyber security skills gaps and shortages which exist in the UK. The findings illustrate the challenges organisations face in recruiting and training cyber staff, as well as the difficulties individuals entering the sector may experience in finding the right career and training pathways.

Several of the headline findings from this year's study are consistent with last year, including:

- The prevalence of technical cyber skills gaps within and outside the cyber sector, including an ongoing lack of basic cyber skills among half of all UK businesses
- The specific skills areas and seniority levels seen as hardest to fill, although there has been an upwards trend in businesses not feeling confident in incidence response year on year
- The number of cyber firms experiencing complementary skills gaps continues to be almost as high as the proportion with technical skills gaps
- A lack of workforce diversity in terms of gender and disability status, particularly in senior roles

Many of the qualitative insights from this year's study also match those from previous years:

- A lack of awareness around professional development pathways, and little or no time or funding for people outside the cyber sector to dedicate to Continuing Professional Development (CPD)
- The perceived cost and benefits of taking on staff at entry-level and the capacity of organisations to train these individuals to the required level. While some organisations regard this as a solution to skills' shortages, others baulk at the time and cost required
- The need for both technical and complementary skills in recruitment. Candidates with both remain highly valued and hard to find

For this reason, the 9 recommendations laid out in our 2021 report still stand, and government and industry should continue their efforts in these areas[26]. In addition, we acknowledge the value of the UK Cyber Security Council's Careers Route Map, which met with positive feedback in our interviews.

Our study provides a comprehensive picture of the supply side and demand side of UK cyber skills gaps and shortages and how the cyber security labour market is evolving. The key insights from this 2023 report are as follows:

- **Demand for cyber security professionals continues to rise, although there were signs of a slow down in the second half of 2022**. Last year saw an increase in job postings and this year there was another rise, with core cyber job postings increasing by 33% and 'all cyber roles' up by 30%. Despite demand somewhat slowing in the latter half of 2022, it remains high compared with historic trends. In the qualitative research, both recruiters and employers described the jobs market as very competitive. The quantitative research found the average number of vacancies per cyber sector firm has risen, standing at 5.2 in 2021, 6.8 in 2022 and 8.2 this year. Our estimate of the cyber workforce gap – the annual shortfall in cyber security personnel – has slightly decreased to 11,100 compared to last year's estimate of c.14,100. This is due to a smaller growth rate of the workforce but the gap remains persistent and annually cumulative in effect

[26] The 9 recommendations for included in our 2021 report are also included in the Annex of this report.

- **New estimates for proportions of the workforce within the cyber sector in specific roles highlight the high prevalence of generalists.** This year, for the first time, the quantitative research estimates the proportion of the workforce within cyber sector firms that carry out each of the cyber security specialisms aligned to the UK Cyber Security Council's Careers Route Map. A majority (61%) of the workforce are cyber security generalists. Beyond this, the distribution of cyber security roles in the sector is not skewed towards one specialism. The preponderance of generalists may be down to a number of factors; the need for staff to sit across multiple specialisms, consultancy roles which require a wide range of familiarity with cyber security or difficulties in classifying staff. If we look at the non-cyber workforce, generalists are the norm, with small teams and 84% of staff transitioning into the role from a non-cyber related role
- **There has been a rise in roles advertised that can be undertaken remotely/from home which could have wide-ranging workforce implications over time.** The workforce could become more widely dispersed and hiring applicants from a wider geographical area may enable the recruitment of more diverse candidates. We estimate that 28% of job postings for core cyber roles had no regional location listed (i.e. the roles were marked as 'Remote' or 'UK-wide'), compared to 21% in 2021 and 13% in 2020. "The company offer is not good enough" is the number one reason employers give for staff leaving roles, and for some staff remote or hybrid working will be an important element of this. We heard mixed views from employers on remote working in the qualitative research, with some saying that remote or hybrid made their organisation a more attractive proposition, while others preferred to have employees in the office. However, if the market continues to be candidate-driven, we may continue to see a rise in remote or hybrid working
- **Training and development present a dilemma for employers in a tight job market.** The qualitative research highlighted the importance of training and development in both attracting and retaining employees. However, once staff achieve new qualifications or certifications, their skills become more valuable and they may seek – or be approached for – higher paid roles elsewhere. We heard of a few examples of organisations repeatedly training people up only for them to leave. This can act as a barrier both to upskilling staff and to taking on staff at entry level
- **There is an upward trend of businesses lacking confidence in their incident management skills.** Among those businesses that do not outsource incident management, 4 in 10 (41%) are not very or not at all confident that they would be able to deal with a cyber security breach or attack compared to 27% in 2020. This may be due in part to perceptions that the threat landscape is becoming more challenging, an issue which some cyber leads have raised in the qualitative research this year and in previous years. This in turn could influence levels of confidence in dealing with cyber attacks
- **Diversity of the workforce is consistent and widening the talent pool remains a key challenge.** The latest study shows that the diversity of the workforce has remained consistent. With gender, the change from 2022 is not statistically significant. In the qualitative research, we heard some argue some progress has been made on diversity, with employers focusing efforts on entry level positions, but much remains to be done. A lack of diverse candidates remains a significant challenge raised in the qualitative research, again highlighting the importance of widening the talent pool. One difficulty here is that the gender gap for cyber security courses remains wide, with only 12% of female graduates at undergraduate level, and 23% at postgraduate level. Another is that, as we have discussed, some organisations prefer to recruit only experienced candidates
- **We heard positive feedback on the UK Cyber Security Council's Career Route Map but awareness is currently low.** Employers and recruiters said it was valuable to have the roles and

specialisms laid out in one place. This could help with recruitment, understanding what skills they currently had in their organisation and potential career progression for their cyber staff. A few were already using it or considering using it to standardise roles. It is important to note that a few cyber leads from outside the cyber sector felt the Route Map was too specialist or even struggled to understand that it related to career pathways rather than cyber security more broadly. It would be beneficial to raise the profile of the Career Route Map (now renamed ‘The Cyber Career Framework’). It has an important role to play in shaping employers’ and individuals’ understanding of possible career pathways into and within the cyber security labour market

Appendix: regional findings summary

Summary of employment and job vacancies metrics by UK region, covering the previous calendar year (2022)[27]

UK region	Number of active cyber sector offices	Percentage of all UK cyber sector offices	Percentage of UK-based cyber sector employment	Number of UK core cyber security job vacancies (where region is known)[28]	Percentage of all UK core cyber security job vacancies	Average (mean) advertised salaries in core cyber security roles
Greater London	1,504	31%	30%	5,966	33%	£71,000
South East	248	5%	6%	1,167	6%	£57,100
North West	456	9%	10%	1,759	10%	£56,800
South West	313	6%	6%	1,065	6%	£56,500
West Midlands	382	8%	8%	1,641	9%	£55,700
East of England	141	3%	2%	417	2%	£55,300
Yorkshire and the Humber	223	5%	5%	1,554	8%	£55,100
Scotland	861	18%	15%	2,338	13%	£54,700
East Midlands	400	8%	7%	991	5%	£54,500
North Eastfconsi	115	2%	4%	336	2%	£53,800
Northern Ireland	189	4%	3%	639	3%	£53,700
Wales	138	3%	4%	450	2%	£52,200
All UK						**£59,400**

[27] The total number of active cyber offices for the UK is 4,970. Regional recruitment data does not include remote working so this is not included in the main report

[28] Based on 18,0328 core cyber job postings on the Lightcast labour insight platform from January to December 2022, where region was listed (out of the total 71,054 core cyber job postings in this period).

Annex- Recommendations from 2021

The following recommendations are all based on the evidence generated in the 2021 year's study. They were also informed by government and industry stakeholders' reflections on this evidence, from the recommendations workshop.

However, given the consistency of the findings across years, the previous recommendations still stand, and government and industry should continue their efforts in these areas.

Once more, progressing these recommendations will require engagement and collaboration from a mix of government, the UK Cyber Security Council, cyber employers, education institutions and recruitment agencies. It is up to government and industry to decide and agree their respective roles. Hence, we generally do not assign responsibility for each recommendation in this way.

Changing attitudes and behaviours

Recommendation 1: 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.[29]

Recommendation 2: 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.

Recommendation 3: 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

Recommendation 4: 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.

Recommendation 5: 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

Recommendation 6: 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.

Recommendation 7: 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.

Recommendation 8: 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.

Recommendation 9: There should be further work to understand how to tackle 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.

[29] This includes, for example, the NCSC Board Toolkit, guidance on home working and guidance on moving from physical to digital business.

Our standards and accreditations

Ipsos' standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a "right first time" approach throughout our organisation.

ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos was the first company in the world to gain this accreditation.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation. We were the first company to sign up to the requirements and self-regulation of the MRS Code. More than 350 companies have followed our lead.

ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.

ISO 27001

This is the international standard for information security, designed to ensure the selection of adequate and proportionate security controls. Ipsos was the first research company in the UK to be awarded this in August 2008.

The UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018

Ipsos is required to comply with the UK GDPR and the UK DPA. It covers the processing of personal data and the protection of privacy.

HMG Cyber Essentials

This is a government-backed scheme and a key deliverable of the UK's National Cyber Security Programme. Ipsos was assessment-validated for Cyber Essentials certification in 2016. Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet.

Fair Data

Ipsos is signed up as a "Fair Data" company, agreeing to adhere to 10 core principles. The principles support and complement other standards such as ISOs, and the requirements of Data Protection legislation.