Cyber security skills in the UK labour market 2022

Findings report

Gabriele Zatterin, Grace Atkins, Alex Bollen and Jayesh Navin Shah, Ipsos
Sam Donaldson, Perspective Economics

Department for
Digital, Culture
Media & Sport

Ipsos

Contents

Summary

This is a summary of research into the UK cyber security labour market, carried out on behalf of the Department for Digital, Culture, Media and Sport (DCMS). 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 with cyber sector businesses and the wider population of UK organisations (businesses, charities and public sector organisations – with this summary focusing on businesses)
- Qualitative research with recruitment agents, cyber firms and large organisations in various sectors
- A secondary analysis of cyber security job postings on the Burning Glass Technologies database, as well as recruitment pool data originating from the Higher Education Statistics Authority (HESA)

This is the fourth iteration of the research, which has been carried out on a roughly 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 697,000 businesses (51%) 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 451,000 businesses (33%) have more advanced skills gaps, most commonly in areas such as penetration testing, forensic analysis and security architecture
- Almost 4 in 10 businesses (37%) 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 4 years of data. By contrast, more businesses this year find themselves lacking incident management skills (up from 27% in 2020, to 32% in 2021 and 37% now).

The qualitative evidence continues to suggest, in line with previous years, that management boards (outside the cyber sector) lack an understanding of cyber security. In particular, the interviews highlight a potential knowledge deficit among c-suite decision makers tasked with overseeing cyber security. This is linked to the absence of a comprehensive generalist training pathway for individuals moving into these positions, and other challenges such as a lack of time to dedicate to cyber security.

Excluding those working directly in cyber sector firms, 85 per cent of the individuals fulfilling cyber roles in the private sector have transitioned into this position from a previous non-cyber role. By contrast, in the cyber sector, more than half the workforce (54%) have previously worked in a cyber role elsewhere.

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

- Half (49%) of all cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants. A total of 19 per cent say that job applicants having these skills gaps has prevented them from achieving business goals *to a great extent*

- Technical skills gaps were most commonly cited in the following 3 areas: incident management, investigation and digital forensics (47% of the firms identifying any technical skills gaps), product development (45%) and assurance, audits, compliance and testing (43%)

The need for complementary skills was also a strong theme in this year's research. Around 4 in 10 cyber sector firms (41%) 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 higher than last year (when it was 31%). In the qualitative interviews, there was an additional emphasis placed on the lack of training and skills around technical report writing and, outside the cyber sector, on influencing the behaviour and culture of staff.

Qualifications and training

Relevant technical training remains much more common among staff in cyber sector firms than among cyber teams in the wider private sector. There is still a narrow set of qualifications and certifications that are most in demand.

- Three-quarters of cyber firms (73%) have provided training for staff in cyber roles in the last 12 months, whereas around 1 in 5 (21%) businesses outside the cyber sector have done so
- Among the 21 per cent of businesses that provided this training, the proportion saying the needs of their cyber staff were met *completely* has fallen this year (to 12%, vs. 20% in 2021)
- Just over 6 in 10 cyber firms (63%) report employing staff who have, or are working towards, cyber security-related qualifications (i.e. in higher education, apprenticeships or other certified training)
- Consistent with the previous 4 years, the most commonly requested certification by cyber employers is Certified Information Systems Security Professional (CISSP), which is in 39 per cent of online job postings in 2021 that ask for a specific certification. Cisco Certified Network Professional and Cisco Certified Network Associate certifications are also in high demand, with 21 per cent of job postings requesting each of these

The qualitative research raised several insights into the challenges faced around training and Continuing Professional Development (CPD) for individuals in cyber roles, including:

- The time taken to attend and deliver training, which could be used for billable work or other core responsibilities, and required a significant time investment across several years for entry-level staff
- A lack of human resources and management capabilities in smaller cyber firms, making it difficult for them to place apprentices in their teams
- Outside the cyber sector, a limited awareness of professional development pathways and relevant training, and a lack of emphasis on CPD for individuals in cyber roles, particularly generalist roles
- The existence of low-quality cyber security training in the external training market, making it challenging to distinguish good and bad training

In response to these challenges, employers were adopting a mix of different styles of training, including self-guided training (largely using external, online courses) work shadowing, mentoring, and structured processes for sharing knowledge internally. The emphasis on mentoring highlighted the perceived importance of longer-form training to help staff build the confidence to apply their technical skills.

It still is uncommon for businesses outside the cyber sector to provide cyber security training for wider staff. Just 1 in 9 (11%) have done so within the last 12 months. While this is more common in larger organisations, only around half of large businesses have done so. Moreover, the qualitative research suggests an ongoing challenge around convincing staff that they need cyber security training.

Recruitment and staff retention

The demand for cyber security professionals has increased significantly since the previous study. On average, there were 4,400 core cyber security postings in each month of 2021 – an increase of 58 per cent from 2020. While there are c.7,500 new entrants into the cyber security labour market each year (according to our estimates), there are also c.4,600 people estimated to be leaving this labour market each year. With the growth in demand for cyber skills, we estimate a total UK cyber workforce gap – the annual shortfall in cyber security personnel – of c.14,100 (vs. the previous year's estimate of c.10,000).

According to our job vacancies analysis, which covers all cyber security online job postings from January to December 2021:

- The most common roles in demand are security engineers (35%), security analysts (18%), security managers (14%), security architects (11%) and security consultants (9%)
- The sectors most in demand of cyber talent are the consultancy, IT (excluding cyber sector firms), and finance and insurance sectors. More cyber sector firms appear to have moved towards indirect recruitment methods (e.g. recruiting via LinkedIn), so account for a smaller share of online job vacancies than in the previous year
- The technical skills areas most in demand are very consistent with the previous 4 years, including information security, network security, skills around ISO 27001. Beyond this, job adverts typically ask for a wide range of specialist skills covering network engineering, risk management and technical controls, operating systems and virtualisation, cryptography, and programming
- There are still geographic hotspots where demand is strongest, in cities like London, Manchester, Bristol and Birmingham. However, our evidence suggests that demand is more regionally spread beyond London this year, most likely as a result of increased remote or hybrid working

The survey and qualitative research also revealed new and recurring insights into the challenges that employers and recruitment agents face when trying to fill cyber security job vacancies:

- In line with last year, recruitment agents said they commonly saw poorly written job specifications – ones that tried to recruit multiple roles in one, were not reflective of the actual requirements for the role on offer, or underplayed important benefits such as training. On this note, the UK Cyber Security Council's Careers Route Map was felt to be a helpful new tool to better match job applicants' and employers' expectations around specific job roles
- The trend towards remote and hybrid working as a result of the COVID-19 pandemic has, in many cases, made employers more agnostic about where their cyber employees are based. The evidence suggests this has led to market rate salaries for cyber roles being equalised across regions, presenting challenges for smaller, regional employers

In the cyber sector specifically, there is evidence of a more challenging labour market from the perspective of employers. More than half of cyber sector businesses (53%) have tried to recruit someone in the previous 18 months.[1] Of all the vacancies over this period, 44 per cent were reported as being hard to fill (up from 35% in the 2020 report, to 37% last year and 44% now).

- The most common reason given for vacancies being hard to fill continues to be around candidates lacking technical skills and knowledge (43% of employers with any hard-to-fill vacancies). This year mentions of competition from other employers have increased (from 9% last year to 25% this year), and more people now mention a general lack of candidates as well (up from 13% to 25%)

[1] This refers to the 18 months before the survey fieldwork, which roughly captures all job vacancies since the start of 2020.

- In 5 in 10 cases (52%), cyber firms have found it hard to fill generalist roles, including senior management roles in their business. The most common shortage in a specialist role is in penetration testing (20% of employers with hard-to-fill vacancies)

At the same time, there are early-stage indications that the cyber sector is increasingly taking on entry-level staff. In 2020, 12 per cent of the cyber workforce in non-large cyber sector firms were new graduates or apprentices (vs. 14 per cent in 2021 and 18 per cent now). Further years of data will help to validate this indicative trend.

Diversity

There is evidence that the cyber sector workforce has become more diverse across the past 3 years, in terms of the number of women and ethnic minorities working in cyber roles – although further years of data will be required to strengthen this evidence. In 2020, we estimated that 16 per cent of the workforce came from ethnic minority backgrounds and 15 per cent was female. The 2022 data shows that:

- People from ethnic minority backgrounds now make up 25 per cent of the sector workforce and 14 per cent of those in senior cyber roles (i.e. those typically requiring 6 or more years of experience)
- 22 per cent are now female, and women make up 13 per cent of those in senior roles
- 10 per cent are neurodivergent, and this group makes up 6 per cent of those in senior roles
- 8 per cent are physically disabled, falling to 3 per cent in senior roles

The proportion of cyber roles going to women remains lower than for other digital sectors (22%, vs. 30% across all digital sectors). However, these figures also highlight the untapped recruitment pool, of people from diverse groups with relevant transferable skills, with the potential to transition into cyber roles.

The qualitative research highlights that workforce diversity has, in general, become a higher profile issue in recent years. However, in some quarters a stereotypical image of cyber roles and relatively passive employer approaches to diversity persist, putting the onus on diverse candidates themselves to be more vocal about their support needs. This year's findings show the importance of having advocates for diverse cyber recruitment, within organisations and across the industry, to help shift the culture among employers and raise awareness of diverse candidates' needs.

Ultimately, these findings highlight an ongoing need for industry-wide initiatives to build diversity in the recruitment pool, encourage employers to cast their nets more widely and ensure they use best-practice recruitment approaches, particularly when recruiting senior roles. Current initiatives in this area include the government's Cyber Explorers platform, the industry-led Tech Talent Charter and the previously mentioned Careers Route Map by the UK Cyber Security Council.

Conclusions

This report on the cyber security labour market is in line with many of the key messages from previous years. This year, on top of the skills, training and recruitment challenges from before, this labour market is undergoing a significant expansion, further straining employers' time and resources after the challenges of the COVID-19 pandemic. The main lessons are as follows:

- Across the economy, it is still common to find skills gaps in basic technical areas. Alongside this, skills gaps around incident management are increasing
- While cyber sector businesses also continue to grapple with technical skills gaps, a lack of complementary skills among job applicants has become a more significant problem this year

- With the increasing demand for cyber skills, it is more important than ever that cyber employers and job applicants understand training needs, and can identify high-quality external training
- There is early-stage evidence of increasing recruitment of career starters and improvement in some aspects of workforce diversity (both in the cyber sector). Further years of data will help to validate both these trends
- The impact of the pandemic continues to be felt by cyber employers and cyber teams. In particular, it may have led to higher market rate salaries outside London and the South East, presenting challenges for smaller, regional employers

1 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. The previous studies were published by DCMS in 2021 (fieldwork in 2020), 2020 (fieldwork in 2019) and 2018.[2]

The 2022 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, qualifications, recruitment 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

In 2021, DCMS published additional research to gather statistics and qualitative evidence on the cyber recruitment pool in the UK. The research focused on the supply of labour and skills, as opposed to the demand-side focus of the above objectives. This year, both these research projects have been brought together. Therefore, this study now also covers:

- Statistics on the size of the UK's cyber security recruitment pool
- An estimate of the overall cyber workforce gap
- Recruitment agents' views of the recruitment pool and how it has changed in the last year

1.2 Summary of the methodology

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 sector firms. These surveys gathered the main estimates on skills gaps and shortages reported in this study. Fieldwork was conducted between 16 August and 19 November 2021.

2. **Qualitative interviews –** Ipsos conducted a more focused strand of qualitative research, with 29 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 and workplace diversity. Interviews took place across October and November 2021.

[2] 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 2021 study, even though the fieldwork was in 2020.

3. **Job vacancies analysis** – Perspective Economics analysed cyber security job postings on the Burning Glass Technologies 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 primarily covered vacancies across the 12 months of 2021, supplementing the work done in the 2021 study (which covered vacancies from September 2019 to the end of December 2020).

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 2022). 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.

1.3 Similarities and differences from the 2021 study

The 2022 methodology is very consistent with previous years, which included strands 1 to 3 in Section 1.2. Strand 4 (the supply side analysis) updates the work done in the 2021 cyber recruitment pool study. This means that the survey, job vacancies analysis and supply side analysis (the quantitative elements) are all able to look at trends over time.

This section summarises the main changes that affect this report (on the main findings). The full details of any methodological changes are included in the separate technical report.

Questionnaire changes

The quantitative survey questions are reviewed and partially revised each year to ensure we capture the metrics that are most useful for DCMS and its stakeholders. This year, we included new questions to break down the cyber workforce by specialism and to categorise the hard-to-fill vacancies that cyber sector businesses face.

Sample sizes

The overall sample sizes achieved for each audience in the quantitative survey broadly match or exceed those from 2021. For large businesses, public sector organisations and cyber firms, we increased the targets this year, giving greater statistical reliability for these groups. This year we interviewed:

- 947 businesses across the private sector (vs. 965 in 2021), of which 107 were large businesses (vs. 65 in 2020)
- 123 public sector organisations (vs. 76 in 2021)
- 211 charities (vs. 220 in 2021)
- 224 cyber firms (vs. 171 in 2021)

The margin of error for the overall business sample is broadly in line with last year, at ±3-4 percentage points.[3] As expected, the margin of error has decreased for large businesses (from ±8-13 percentage points in 2021 to ±6-10 percentage points in 2022), public sector organisations (from ±7-12 points to ±5-9 points) and cyber firms (from ±4-7 points to ±4-6 points).

[3] The margins of error are confidence intervals at the 95% significance level, using the effective sample size. The effective sample size is a measure of the statistical reliability of samples that takes into account any sample manipulation such as weighting. A margin of error range is displayed here, because the actual margin of error will vary depending on the specific survey result under consideration.

Removal of requirement to produce recommendations

In previous years, this study was used to produce a set of specific recommendations for the government and industry around tackling the cyber security skills gap. To this end, Ipsos carried out a workshop with key stakeholders from government, industry and academia following the other strands of the project, so that these stakeholders could contribute to the project's recommendations.

DCMS agreed that the recommendations from previous years remained relevant and important, so there was no requirement to produce further recommendations this year.

1.4 Differences from other recent studies looking at cyber security skills

ISC2 is a global membership organisation for cyber security professionals. It publishes an annual Cybersecurity Workforce Study, the most recent of which was published in November 2021. This is a study of the global cyber security workforce and largely reports its findings at a global level.

The findings from the ISC2 2021 report touch on similar themes to our study (such as skills gaps, diversity in the cyber sector, qualifications and the ongoing impact of COVID-19) but they are not directly comparable. This is also the case for other well-known surveys that have been published around the same time period, the National Cyber Security Centre (NCSC)/KPMG Decrypting Diversity 2021 report and the PwC Cyber Security Strategy 2021 report.

- Our primary research is UK-specific and has a large sample size. This means we can break down findings for UK organisations by size and sector. Other surveys have often not been able to be so granular and have typically reported findings for Europe as a whole, rather than the UK

- Our survey results are sampled and weighted to be representative of organisations of all sizes and sectors. This includes micro and small businesses, and low-income charities, that may be less aware of their cyber security skills needs and make up the vast majority of all businesses and charities in the UK. The ISC2 and PwC surveys appear to have been carried out online with a self-selecting sample, skewed towards the largest and most engaged organisations. These studies are important, as they have good coverage of the organisations with the most sophisticated cyber security skills needs. However, they are not necessarily representative, and typically omit micro, small and medium businesses, and the charitable sector, where there are often more basic cyber security skills needs

- Our cyber sector diversity statistics are also intended to be representative, as they are based on workforce-level data collected from a random sample of UK cyber firms. This is very different to the NCSC/KPMG survey, which is again undertaken online with a self-selecting sample that may be subject to clustering effects (depending on where and how the survey was promoted). There is also value in the NCSC/KPMG results, which serve to highlight the lived experiences of diverse groups within the cyber security workforce. However, these results, unlike our study, cannot be used to reliably infer the incidence of characteristics in the wider population

- This research measures skills gaps – the number of organisations lacking specific cyber security skills – in a particular way. As we cannot objectively test whether organisations are capable of carrying out specific cyber security tasks involving specialist skills, we instead ask about their confidence at being able to carry out a range of these tasks (see Chapter 4 for full details). This continues the methodology from the 2 previous studies

1.5 Interpretation of the data

Charting of survey results

Where figures in charts do not add to 100%, this is typically due to rounding of percentages that come from weighted data, or because the questions allow more than one response.

In stacked bar charts with bars showing values under 3 per cent, we have opted, for visual clarity, to leave these bars unlabelled.

Subgroup analysis

For businesses, analysis by size splits the population into micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more). For charities, we consider size in terms of annual income band. However, with some exceptions, there are too few public sector organisations and charities sampled to split out results by size or income band across most of the results.

In our sector subgroup analysis, we grouped similar sectors together by SIC 2007 code for higher sample sizes. The groupings are the same ones used in DCMS's Cyber Security Breaches Survey series. Ultimately, there are relatively few major sector differences that we report on, but this is the full list of sector groupings that we looked at in the subgroup analysis:

- Administration or real estate (SIC L or N)
- Construction (SIC F)
- Education (including academies) (SIC P)
- Entertainment, service or membership organisations (SIC R or S)
- Finance or insurance (SIC K)
- Food or hospitality (SIC I)
- Health, social care or social work (including NHS organisations) (SIC Q)
- Information or communication (SIC J)
- Professional, scientific or technical (SIC M)
- Retail or wholesale (including vehicle sales and repairs) (SIC G)
- Transport or storage (SIC H)
- Utilities or production (including manufacturing) (SIC B, C, D or E)

Typically, we compare each sector to the average private business. The education sector and health, social care or social work sectors include a mix of private and public sector organisations. We therefore compare these sectors to a merged sample of private and public sector organisations, specially weighted to represent a merged population profile.

The quantitative survey found few noteworthy or consistent regional subgroup differences. Therefore, we have typically not commented on these across the report. We do, however, have a far more substantial geographic analysis as part of strand 3, the secondary analysis of job vacancies (covered in Chapter 7).

Statistical significance (for subgroups and changes over time)

The survey results are subject to margins of error, which vary with the size of the sample and the percentage figure concerned. We carry out statistical significance tests, which signify whether differences across the results are likely to be real differences in the population, or likely to have occurred by chance.

In this report, where we highlight any subgroup differences by business size or sector, or any other variable, these are statistically significant differences (at the 95% level of confidence) – unless the commentary states otherwise. Similarly, where we indicate that findings have changed since the previous studies, this is indicating a statistically significant change over time unless otherwise stated.

Specifically, this report contains several *workforce*-level estimates compiled from *employer* survey data. They estimate the percentage of the cyber workforce with certain traits (e.g. the proportion of the cyber sector workforce that is female), unlike most of the reported data which represents the percentage of employers. We do not expect to find statistically significant differences over time in these estimates given sample size limitations. Instead we focus on broad trends and patterns in the data.

Interpreting qualitative data

The qualitative findings offer more nuanced insights and case studies into how organisations address their cyber security skills needs, and why they take certain approaches. The findings reported here represent common themes emerging across multiple interviews.

Where we pull out an example, insight or quote from one organisation, this is typically to illustrate findings that emerged more broadly across multiple interviews. As with any qualitative findings, these examples are not intended to be statistically representative of the wider population of UK organisations.

1.6 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 and participation at the action-planning workshop.

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

2 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. Just like in the 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 all businesses (50%) have just 1 employee responsible for cyber security. Larger organisations continue being slightly better resourced, although even in these organisations, cyber teams of more than 5 people are very rare
- Within the cyber sector, more than half of the cyber workforce (54%) entered their current job after being employed in a previous cyber role. By contrast, outside the sector, the staff performing cyber duties in-house are overwhelmingly transitioning from a non-cyber role (85%)
- A quarter of the cyber workforce are cyber security generalists (26%), while 14 per cent work in governance, risk and compliance (GRC) role and the remaining 60 per cent are technical specialists in specific areas
- There are indications that the non-large firms in the cyber sector are increasingly taking on entry-level staff, although only 19 per cent of all cyber firms currently do this

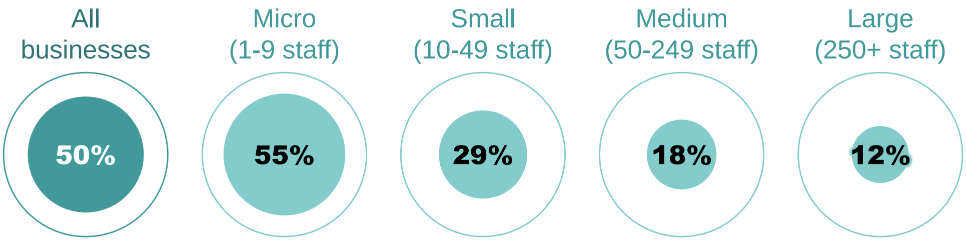
2.1 Size of cyber teams

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. Half of businesses (50%) and two-fifths of charities (41%) 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 just under a fifth (17%) having only 1 person in this role.

As Figure 2.1 shows, organisations tend to expand their cyber teams as they grow. Among both medium and large businesses, the typical (median) cyber team comprises 2 to 3 people. Just under a fifth of medium businesses (17%) and a quarter of large businesses (23%) have 4 to 5 people in these roles.

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



Bases: 947 businesses; 442 micro; 248 small; 150 medium; 107 large

These results are generally very consistent across sectors.

The businesses that outsource any aspects of cyber security tend to have better-resourced in-house cyber teams than those who do not. Three-fifths (60%) of those that outsource have more than 1 person responsible, compared to two-fifths (43%) of those who do not outsource. This suggests that outsourcing continues to be used by organisations as a way of expanding their cyber capacity, rather than as a way of replacing their in-house cyber security staff.

All these patterns are consistent with all 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.

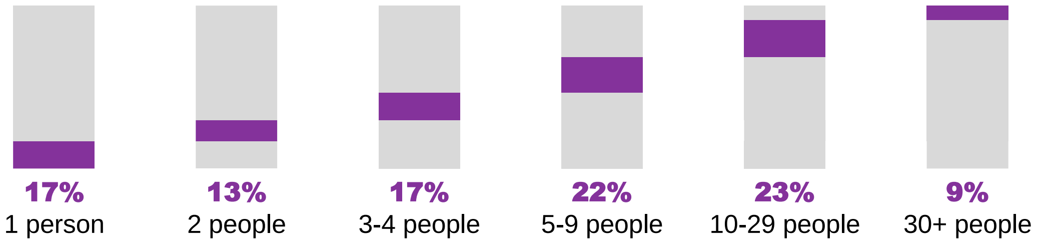
Cyber teams within the cyber sector

Most firms in the UK cyber sector (i.e. those trading in cyber security products or services) continue to be smaller businesses. The DCMS Cyber Security Sectoral Analysis 2022 finds that 57 per cent of these firms are micro and 24 per cent 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).

The latest Cyber Security Sectoral Analysis does highlight a slight overall increase in the proportion of small businesses operating in this sector (with 10 to 49 employees across all roles). Our survey suggests there has specifically been an increase in the businesses with 10 to 29 employees in cyber roles (from 14% last year to 23% this year).

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



Base: 223 cyber sector businesses (i.e. excluding 1 from the full sample that did not provide this information)

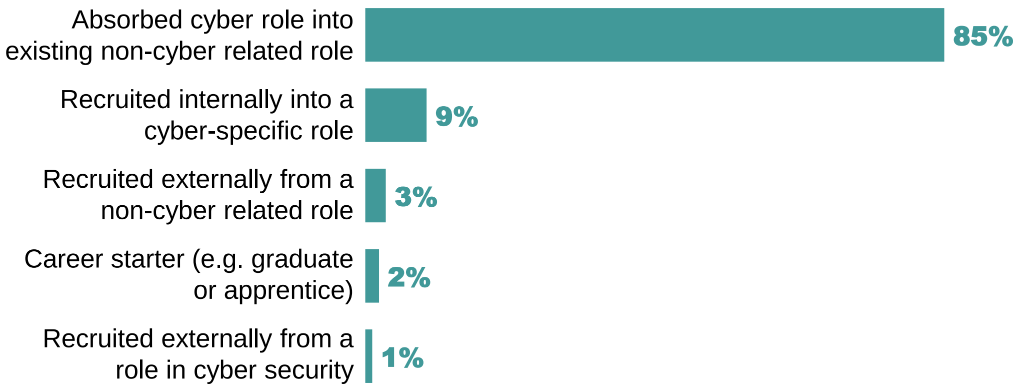
2.2 Career pathways into cyber roles

Career pathways into cyber roles outside the cyber sector

Among all the staff carrying out any cyber functions in the private sector, more than 8 in 10 have absorbed these tasks into an existing non-cyber related role (Figure 2.3). In these roles, cyber security may not be their only or top priority.

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. A negligible proportion of the workforce entered their current role in this way (our estimate is around 1% across all businesses, rising to 7% within medium and large businesses). These findings are in line with those from the 2021 study. They suggest 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



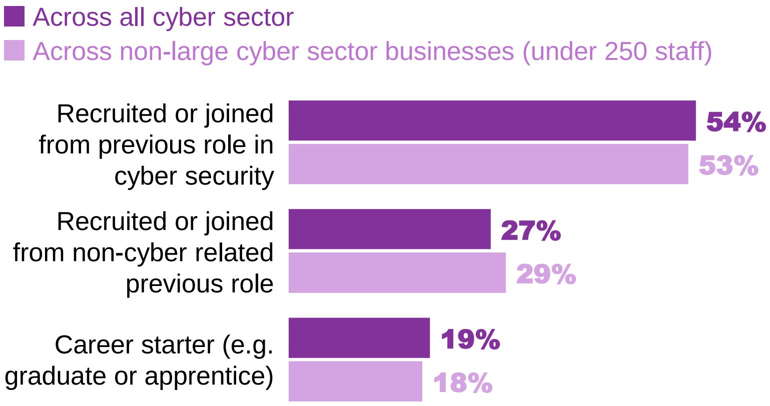
Bases: c.870 businesses (where answers given on team size and on how each individual came into the team)

Career pathways within the cyber sector

Within the cyber sector, more than half of the cyber workforce entered their current role after working elsewhere in a cyber role (54%). 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 (27% vs. 19%). In previous years, our findings indicated that large businesses in the cyber sector disproportionately took on graduates and apprentices, more so than smaller firms. However, the emerging pattern across 3 years of data suggests that a wider range of employers are taking on career starters than before – in 2020, 12 per cent of the cyber workforce in non-large cyber sector firms were new graduates or apprentices (vs. 14 per cent in 2021 and 18 per cent now). Further years of data will help to validate this indicative trend.

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



Bases: 214 cyber sector businesses (excluding those that could not break down their workforce); 212 non-large cyber sector businesses (under 250 staff)

Are internships or work placements offered in the cyber sector?

Around 1 in 3 cyber firms (27%) reported offering any internships or work placements since the start of 2020 (roughly over an 18-month period). This is almost the same as last year (28%), when this question was first asked.

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

The UK Cyber Security Council is a self-regulatory body for the UK's cyber security profession. The Council is developing 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.

In the qualitative interviews, there was typically very positive feedback on the Route Map (which interviewees were directed to before the interview). Employers and recruitment agents regarded it as a credible and impressive tool, pulled together by experts.

"Whoever has written this either knows a penetration tester or has been one."
Cyber sector business

Employers and recruitment agents saw various applications for the tool. One cyber lead outside the cyber sector suggested that the examples in the Route Map could be used to sell the idea of further training and development to their senior managers. Another said it would help them to update the job specifications for their IT team to include specific cyber security functions and accountabilities. On this note, it was felt to be important to show how the cyber specialisms in the tool aligned to existing IT roles, to avoid organisations outside the cyber sector having to revamp their existing team structures.

Another challenge raised was around ensuring that the Route Map was perceived as relevant to individuals who currently oversaw their organisation's cyber security outside the cyber sector, and therefore required cyber skills, but who did not see themselves as cyber professionals (e.g. IT directors).

Recruitment agents felt the Route Map would be more useful for job applicants than for the hiring managers they worked with. It could help guide applicants to the right training or help them market their existing skills and experience. One recruiter said they would maybe share it with clients who asked for help with their job specification, but they were cautious about coming across as patronising, by implying that clients did not already know their own needs.

"I think this would be particularly useful to candidates, as it would encourage them to see that their background and experience can be helpful."
Recruitment agent

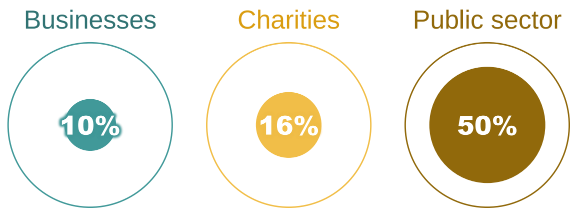
One interviewee highlighted that the Route Map and its current 16 specialisms would need to be kept under constant review, to ensure it captured emerging technology in cyber security. They gave the use of blockchain technology as an example that could be a distinct specialism.

2.3 Are cyber roles labelled as such across UK organisations?

All the previous studies in this series have found that a large proportion of organisations only have staff who carry out cyber functions informally. That is, these functions are not a formal part of their job descriptions and may be a small part of their overall job role. They may also come from non-technical backgrounds, such as general management, legal or human resources teams.

This remains the case in 2022, with no consistent shifts in these results across years. As Figure 2.5 shows, 10 per cent of businesses have formalised their in-house cyber role. This is slightly higher among charities (16%) and substantially higher among public sector organisations (50%), repeating another pattern seen in all previous years.

Figure 2.5: Percentage of organisations where the cyber security role is included in job descriptions



Bases: 947 businesses; 211 charities; 123 public sector organisations

A higher proportion of medium (21%, vs. 10% overall) and large businesses (34%) include cyber security in staff job descriptions. This is also more common in finance and insurance firms (20%), and information and communications firms (18%) – both sectors that have scored more highly at this question in previous years. It is also more likely across schools and other education institutions, from both the public and private sectors (23%). Nevertheless, even amongst these size bands and sectors, most businesses still do not have cyber security responsibilities as a formal part of their job descriptions.

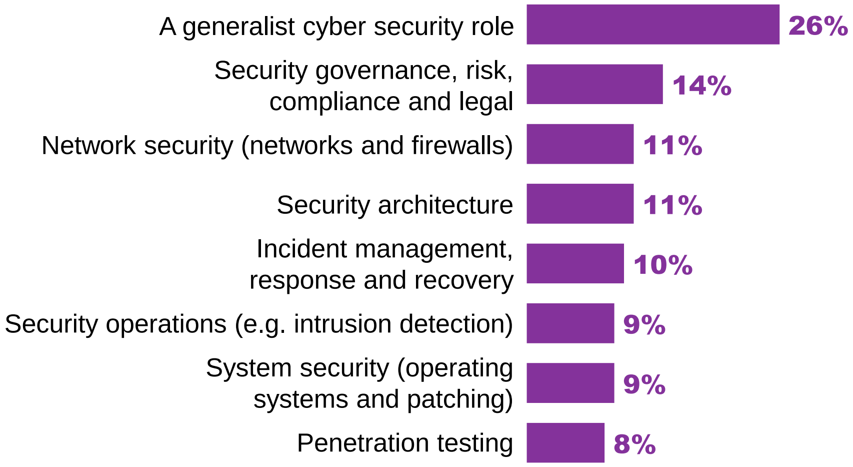
2.4 Specialisms of those in UK cyber sector firms

This year, for the first time, the survey estimates the proportion of the cyber workforce within cyber sector firms that carry out particular cyber security roles. The list of roles (shown in Figure 2.6) reflects DCMS's own categorisation, which aligns to the work of the UK Cyber Security Council and the Cyber Security Body Of Knowledge (CyBOK). Each member of the cyber workforce has been assigned to just 1 of these 8 categories, based on their employer's assessment of their role. If people undertake tasks in multiple categories, we have asked employers to specify the 1 area where they spend most of their time.

These new statistics highlight the high prevalence of cyber security generalists, who make up a quarter (26%) of the cyber workforce in the sector. These are people that, in the view of their employers, are not specialised in any of the other 7 categories noted in Figure 2.6.

Beyond these generalists, the distribution of cyber security roles in the sector is not especially skewed towards one specialism. The next top response is security governance, risk, compliance and legal roles (14%). On the other hand, the remaining 60 per cent of the cyber workforce are technical specialists – they do not work in a generalist cyber security role nor in a governance, risk and compliance (GRC) role – and these individuals together make up the majority of the sector workforce.

Figure 2.6: Percentage of cyber sector workforce who work in particular roles or specialisms



Base: 209 cyber sector businesses (excluding those that could not break down their workforce)

2.5 Qualifications of those in UK cyber sector firms

Prevalence of different types of cyber security qualifications

Given the fact 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. There is, perhaps, a greater expectation that staff in cyber sector firms, where cyber security is a core product or service, should have the requisite technical knowledge for their jobs.

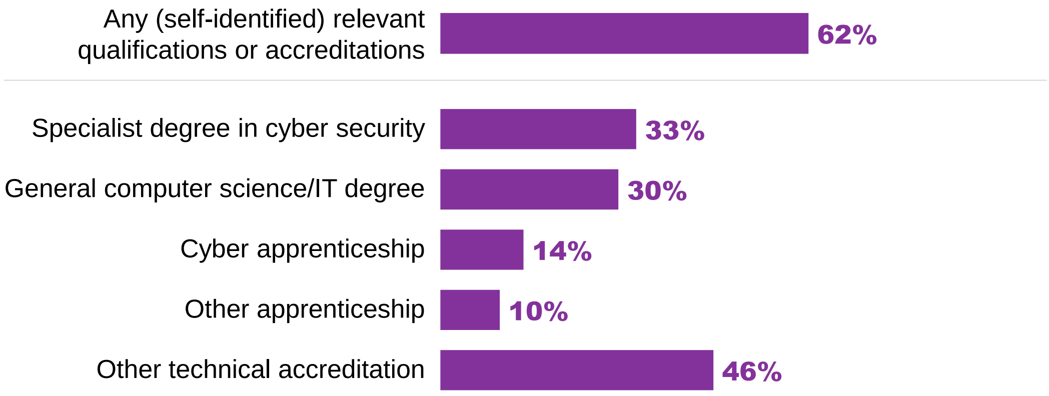
In 2022, just over 6 in 10 cyber sector firms (62%) say that they have any employees with, or working towards, a cyber security-related qualification or certified training. This is less than in 2021 (70%), but in line with the 2020 study (62%). It indicates no clear trend upwards or downwards over the last 3 years. A potential reason for the drop from last year is the entry of several new firms into the cyber sector this year, which has grown from 1,483 firms in 2021 to 1,838 active firms in 2022 according to the latest Cyber Security Sectoral Analysis.

Figure 2.7 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 62 per cent that say their staff have any relevant qualifications or accreditations. When combining the specific responses in the chart, around 4 in 10 (42%) say they have any staff with a relevant higher education degree (in cyber security or computing), and 2 in 10 (19%) have any apprentices among their staff.

The drop from last year (from 70% to 62%) is, by and large, because fewer firms have staff with computer science or IT-related degrees (down from 41% in 2021 to 30% in 2022). Previously, the proportion of cyber firms saying they had staff with general computer science or IT degrees tended to be higher than the proportion saying they had people with specialist cyber security degrees. With the drop in the former, these proportions are now, for the first time, more evenly matched.

There continues to be a great deal of emphasis in the cyber sector on cyber security-specific technical accreditations. Nevertheless, these are often combined with other qualifications across the workforce. For example, among the 46 per cent of employers that have staff with technical accreditations, two-thirds (67%) also have staff with at least one of the types of higher education degrees covered in Figure 2.7.

Figure 2.7: Percentage of cyber sector firms that have staff with the following types of qualifications or accreditations



Base: 224 cyber sector businesses

Chapter 7 covers the specific types of technical accreditations that are most frequently mentioned in job postings, highlighting the extremely wide range of accreditations available in this sector.

Perceptions of cyber security qualifications

In the qualitative research, cyber security qualifications were considered useful or even essential in certain contexts. Service Level Agreements with large business or public sector clients often specified that staff needed to be certified to a certain level. This was felt to be especially common in the security testing specialism. For example, recruitment agents highlighted that this was a particularly strong driver for firms seeking the Certified Ethical Hacker and CREST certifications. One cyber sector interviewee highlighted more generally that possessing relevant qualifications provided a level of quality assurance in very technical areas such as penetration testing and auditing.

However, outside of these technical areas, there was a great deal of scepticism around qualifications, helping to explain why around 4 in 10 firms in the cyber sector do not have staff with relevant cyber security qualifications. The scepticism generally fitted into 3 broad themes:

- Employers often noted that qualifications did not do a good job at signalling the kinds of attributes they were truly interested in among job applicants. This included an aptitude for fast learning and self-learning, problem solving and communication skills. In line with previous years, there was a broad sense that cyber security qualifications were no guarantee of aptitude in a workplace. One cyber sector interviewee noted that, on the contrary, finding someone *without* qualifications who could demonstrate self-taught programming skills often suggested the right mentality to them

  > ***"I interview lots of candidates – I look at experience and the way they talk about it, rather than the qualifications they have. I would love for qualifications to be important, but it's really not the thing we focus on."***
  > *Cyber sector business*

- There were also ongoing concerns, reflected in previous years, about further and higher education courses and modules in cyber security being outdated. For instance, we spoke to one penetration testing firm that had carried out a day-long workshop at a local university in 2020, and lamented that the software used on the course was 5 years out of date

- There was a sense that certain specialisms, like security architecture, were too holistic to be taught and certified in a short space of time. This was coupled with scepticism about the training market. A common perception was that the market was awash with short and cheap training courses, enabling people to receive a certification without investing significant time and effort in the training. This made it challenging for employers to assess the value of qualifications among job applicants

> ***"If you want people to develop abilities in, say, security architecture … it would have to be several seminars over a period of time, rather than just listening to a course for a week, doing a multiple-choice exam and getting a badge."***
> *Cyber sector business*

Attitudes towards a potential Chartered status for cyber professionals

The pros and cons of a Chartered status for individuals working in cyber security roles have been recently discussed, for example in a UK Cyber Security Council blog post from December 2020. In the qualitative interviews, this idea met with a mixed reception. There was a suggestion that offering a training pathway towards Chartered status could help employers with staff retention. Another employer suggested it would act as a kitemark, to help screen job applicants. However, there were also several distinct challenges raised around how Chartered status would work in practice:

- A key consideration would be whether Chartered status is based on someone's breadth of knowledge across different areas of cyber security or their depth of knowledge in particular specialisms. According to one interviewee, the former would only attract employees at more junior levels whereas the latter would create a very narrow pool

- There were concerns about Chartered individuals promoting their status unduly, to claim cyber security expertise outside of their specialism. This was raised as a potential problem for organisations trying to recruit Chief Information Security Officers – since job applicants for these roles tended to come from a wide range of career pathways, they could often be deficient in one or more aspects of cyber security that had not featured in their previous roles

- There was some uncertainty as to how Chartered status would differentiate itself from existing accreditations such as the Certified Information Systems Security Professional (CISSP) or CREST certifications. Some were worried about a Chartered status adding to the existing plethora of accreditations to create further barriers to entry into cyber roles, especially for those transitioning from technical non-cyber roles (e.g. software engineers)

- One interviewee suggested that Chartered status should encompass work experience and not just qualifications, because it would otherwise suffer from the same drawbacks as existing qualifications (discussed earlier in this section)

3 Diversity in cyber security

This chapter covers diversity in the cyber workforce, with an emphasis on gender, ethnicity, physical disability and neurodiversity[4]. 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 businesses 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

- There is evidence that the cyber sector workforce has become more diverse across the past 3 years, both in terms of gender (22% are women, vs. 15% in 2020) and ethnicity (25% are from ethnic minority backgrounds, vs. 16% in 2020)
- 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 13 per cent of senior roles are filled by women
- There has been an increase in efforts to recruit people with neurodiverse conditions (23% of cyber sector employers have made changes for this group vs. 15% in 2021). However, it remains a minority making adaptations to encourage any of these diverse groups to apply

3.1 Estimates of diversity in the cyber sector

All-workforce statistics

There is evidence that the overall diversity of the cyber sector, in terms of gender and ethnicity, has improved over the course of the last 3 years. 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. On this basis, the proportion of the workforce that is female has increased (from 15% in 2020, to 16% in 2021 and 22% in this latest survey) and the proportion from ethnic minorities has also increased (from 16% in 2020, to 17% in 2021 and 25% in this latest survey).

The full quantitative findings in Figure 3.1 show that sector diversity can be continually improved. The cyber sector remains behind other digital sectors with regards to gender diversity – although this highlights an untapped recruitment pool, of people from diverse groups with relevant transferable skills, with the potential to transition into cyber roles. Our estimates are more in line with other digital sectors when it comes to diversity of ethnicities and physical disability, although the latter is slightly behind the wider UK workforce estimate.[5] This overall pattern is unchanged from previous years.

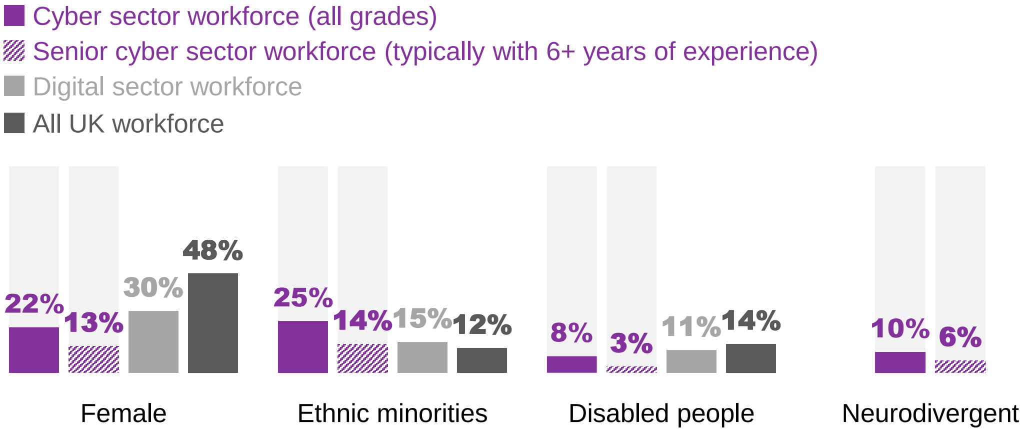
[4] For this study (e.g. in question wording), we defined neurodiversity as the inclusion of people with conditions or learning disorders such as autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD).

[5] Gender, ethnicity and physical disability comparison data comes from DCMS Sector Economic Estimates 2021: Employment 2019–June 2021. We use the July 2020 to June 2021 data.

It is important to note that these estimates are very variable. For example, if we remove the 2 largest businesses from the cyber sector sample, the proportion of female workers falls from 22 per cent to 17 per cent. For ethnic minority workers it falls from 25 per cent to 19 per cent. Therefore, more years of data are required to validate the suggestion that diversity has increased.

A total of 1 in 10 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.

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



Bases: c.200-220 cyber sector businesses for all workforce estimates
(in each case excluding those that were not able to answer these questions, or refused)

We acknowledge that these estimates are very different to those reported in the NCSC/KPMG Decrypting Diversity 2021 report. In their survey, a much higher proportion of respondents identified as female, disabled and neurodivergent. However, while their survey is useful to understand the lived experience of people from these excluded groups, it is not designed to produce figures that are representative of the entire cyber workforce. We consider our figures to be representative.

The NCSC/KPMG survey also does not produce evidence to suggest that gender and ethnic diversity has improved over time, underlining the point that this hypothesis needs further validation in future years.

Senior workforce statistics

Figure 3.1 also contains our estimates for the proportion of the senior cyber workforce that come from these typically excluded 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 per cent come from ethnic minority backgrounds (vs. 25% of the total cyber workforce)
- 13 per cent of the senior cyber workforce is female (vs. 22%)
- 6 per cent are neurodivergent (vs. 10%)
- 3 per cent are disabled (vs. 8%)

These statistics were first collected in 2021, and across all 4 groups there are no notable changes from last year. This suggests that the efforts and initiatives to improve workforce diversity to date may have had more of an impact on junior roles (in terms of improvements in gender and ethnic diversity) than senior ones. It may also reflect that improving diversity among the senior workforce is, in general, more of a challenge than for junior roles – this was raised in last year's report.

Where is diversity seen to be worse?

In the qualitative interviews, achieving diversity was seen to be more challenging in certain situations:

- In senior positions, where the talent pool is narrower (complementing the survey findings)
- In non-client facing roles (e.g. in penetration testing), where there is seen to be less external benefit in demonstrating you are diverse employer
- In roles where freelancing is common (e.g. in cyber security training roles), as incomes are less consistent, creating a barrier to entry for those from less affluent backgrounds
- Where diversity characteristics are not easily observed or measured (e.g. in terms of socioeconomic backgrounds or neurodiversity)

3.2 Attitudes towards workforce diversity

The qualitative interviews highlight that the overall topic of workforce diversity has become more prominent among employers now than 2 years ago, particularly in terms of gender and ethnicity. For example, in some cases outside the cyber sector, organisations had implemented new diversity training at a corporate level. However, these initiatives could sometimes overlook diversity in IT and cyber teams.

Across the board, among both recruiters and employers, there was a sense that more could be done to counteract stereotypes and address negative attitudes towards diversity in these roles.

"There is definitely scope to get new recruits in, younger, older, from different backgrounds and with different experiences that can bring something else to the table."

Cyber sector business

One recruiter pointed out that cyber security careers were often seen as inflexible, with a bias in favour of full-time roles and long or unsociable working hours.

Moreover, outside the cyber sector, there was often a disconnect between human resources (HR) teams and cyber teams when it came to diversity issues. This sometimes led to well-intentioned efforts to improve diversity having negative or contrary outcomes. Recruitment agents noted that whenever they received diversity requirements, these tended to come from HR, were focused on gender, and did not commonly have contributions from hiring managers. In one example, a recruitment agent described how an organisation's cyber team had already identified a preferred candidate for a job, but the agent was asked to find an additional female candidate to interview, solely to meet HR diversity requirements.

"It feels more like a box-ticking exercise, rather than understanding the benefits. I ask them why they want women, and they can't answer that question. They just say, 'HR want more women'."

Recruitment agent

With other aspects of diversity, such as neurodiversity, the picture was more mixed. This year, various interviewees from the cyber sector were spontaneously raising this term in interviews, suggesting a heightened awareness. However, there were still employers that had not considered this diversity characteristic at all, placing it behind gender and ethnicity in terms of its profile.

3.3 Diversity in recruitment processes

More than half of cyber firms (53%) have tried to recruit people into cyber roles since January 2020 – our survey focused on activity over roughly the last 18 months before the interview.

Among this group, a minority report having adapted their recruitment processes or carrying out any specific activities to encourage applications from diverse groups, although the figure for people with neurodiverse conditions has increased. Specifically:

- Four in ten (39%) say they have made changes to recruit more women
- A quarter (27%) made changes for people from ethnic minority backgrounds
- A similar proportion (23%) did so for people with neurodiverse conditions or learning disorders (vs. 15% in 2021)
- One in five (21%) did so for physically disabled people

What are employers and recruitment agents doing to improve diversity?

In the qualitative interviews, the examples of actions taken to improve diversity in cyber security recruitment and teams included:

- Rewording job adverts to be gender-inclusive, sometimes running them through online tools such as Gender Decoder to identify biases
- Offering flexible working
- Recruiting from across the UK – the COVID-19 pandemic was expected to improve workforce diversity by making it the norm for cyber teams to recruit beyond their headquartered regions
- Receiving blind CVs that exclude names and demographics
- Providing English language and pronunciation training
- Implementing mandatory diversity and inclusion training

In other words, these were not necessarily activities specific to cyber roles. Some approaches, such as blind CVs, reflect more general good practice considerations in recruitment across a wide range of jobs.

Another common theme across interviews was the importance of cyber security advocates within businesses and across the industry. The organisations that had taken the types of actions listed above tended to have senior individuals who spoke passionately about diversity in cyber roles and who made a point of highlighting their commitment to greater diversity. One had a diversity and inclusion working group to discuss these sorts of issues across all levels of the business. Another talked about being inspired by Emma Philpott, the Chief Executive Officer of the IASME Consortium, who set up a scheme to train neurodiverse unemployed people in cyber security.

Recruitment agents highlighted that, in their experience, employers were very accommodating when job candidates were open about their needs. However, the current situation often put the onus on candidates themselves to be more vocal with employers about their support needs.

"Employers are quite sensitive about these things, and the last thing they want is for someone to be going around saying they were politically incorrect or made someone feel marginalised. They make quite an effort from what I can see."

Recruitment agent

Nevertheless, various employers, including those that had not taken any of the above steps, remained of the view that there was little they could do to improve diversity in cyber teams. They felt that, ultimately, the problem was in not receiving job applications from candidates with more diverse backgrounds, due to a lack of diversity within the recruitment pool. This highlights the ongoing importance of industry-wide initiatives to build diversity in the recruitment pool, including early interventions like the Cyber Explorers platform, that seeks to inspire young people to go into cyber careers, and the UK Cyber Security Council's previously mentioned Careers Route Map, which aims to support individuals with transferrable skills to transition into cyber roles.

One large cyber firm did suggest that they could do more themselves, by reaching out directly to schools and colleges. However, they noted that this kind of outreach work had typically been done by individuals – some of their employees were science, technology, engineering and mathematics (STEM) Ambassadors for BCS (formerly the British Computer Society) – rather than at a corporate level. This shows the importance of industry-led initiatives like the Tech Talent Charter, that commits signatory organisations at a corporate level to improving and maintaining their diversity and inclusion efforts.

4 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 6.

Key findings

- Half (51%) 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 697,000 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 451,000 businesses
- Half of all cyber sector firms (49%) have faced problems with technical cyber security skills gaps in the past 12 months, either among existing staff (20%) or among job applicants (45%). This year (compared to 2021), there are higher skills gaps in the areas of operational security management and implementing secure systems
- A total of 4 in 10 cyber sector firms (41%) have experienced a complementary skills (or soft skills) gap in this timeframe. This is an increase from last year (when it was 31%)

4.1 Technical skills gaps outside the cyber sector

In line with the 3 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 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.

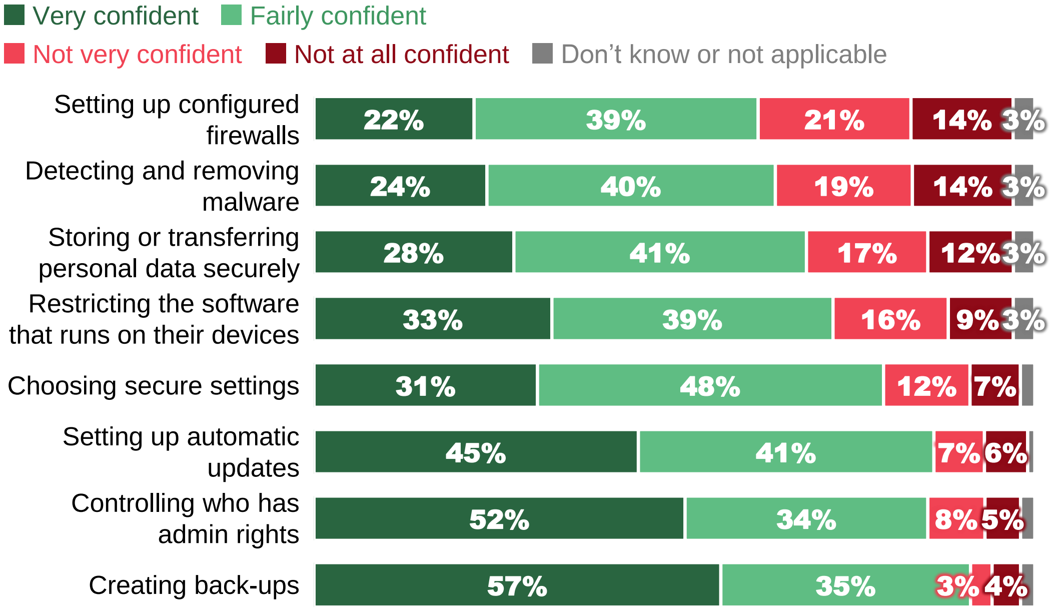
Basic technical skills gaps

The survey explores organisations' ability to confidently cover a range of basic technical cyber security tasks and functions. These tasks, listed in Figure 4.1, have remained consistent across all 3 years of this study. They are a combination of the technical areas covered under the government-endorsed Cyber Essentials scheme[6] and other basic aspects of cyber security highlighted by DCMS.

The areas where skill gaps are most prevalent are in setting up configured firewalls, storing or transferring personal data, detecting and removing malware, and restricting software that runs on business-owned devices. These areas have been at the top of this list in all previous years as well. Nevertheless, only a minority of cyber leads across the business population say they are not confident in carrying out each of these tasks.

[6] 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).

Figure 4.1: Extent to which businesses are confident in performing basic cyber security tasks (where such tasks are not outsourced)

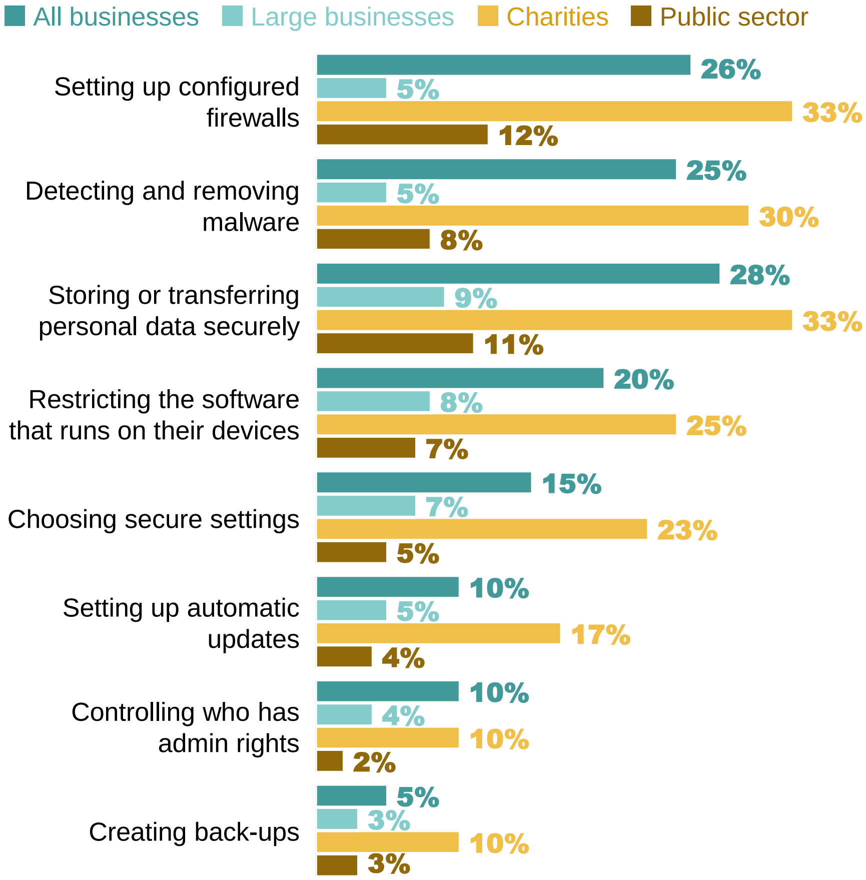


Bases: c.600+ businesses that do not outsource each task
Unlabelled bars are under 3%.

Figure 4.1 does not include businesses that outsource these tasks or functions, as by definition 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 compares this to large businesses, charities and public sector organisations.

Across all these areas, large businesses and public sector organisations are much less likely to report skills gaps. In previous years, charities have been more likely than businesses to express these skills gaps. 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. When specifically comparing large businesses (250 or more employees) and high-income charities (with an income of £500,000 or more), we found that the latter are more likely to lack confidence dealing with cyber incidents – although this difference was based on relatively small sample sizes for each group.

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



Bases: 947 businesses; 107 large businesses (with 250+ staff); 211 charities; 123 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.60+).

These figures have fluctuated across all 4 years of this study series, although there is no clear upwards or downwards trend. This year's data suggests that these basic skills gaps are still on a par with those first measured in the 2018 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.

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 8 tasks listed in Figures 4.1 and 4.2, to get the overall percentage of organisations that are not confident in carrying at least 1 of these basic tasks. From this, we calculate that 51 per cent of businesses have a basic technical cyber security skills gap. Reflecting a pattern from previous years, this estimate is higher for charities (59%) and lower for public sector organisations (24%).

The basic cyber security skills gap is lower for large businesses (21%) and high-income charities (32% of those with £500,000 or more in annual income), indicating that smaller organisations face the greatest difficulty in meeting these basic cyber security requirements.

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 51 per cent to the overall population of private sector businesses, we estimate that approximately 697,000 businesses in the UK have a basic technical skills gap.[7]

Knowledge of basic technical terms

The government-endorsed Cyber Essentials scheme also contains a basic checklist for organisations to follow. As well as instructing organisations to implement basic technical controls, this checklist also highlights 2 basic areas that everyone working in a cyber role should understand, around configured firewalls and sandboxed applications. Our survey shows that:

- While most organisations may claim to feel confident at setting up configured firewalls, there is still a substantial knowledge gap around the basics of firewall management. Those responsible for cyber security in under half of all businesses (44%) and charities (46%) say they understand the distinction between personal and boundary firewalls very well or fairly well. This is substantially higher in medium businesses (65%), large businesses (85%) and public sector organisations (70%). This suggests that our figure of a 26 per cent skills gap for configured firewalls (from Figure 4.2) is likely to be a bare minimum estimate

- In around a quarter in businesses (23%), 3 in 10 charities (30%) and 7 in 10 public sector organisations (70%), those responsible for cyber security say they understand what a sandboxed application – an application that can run with restricted access to the rest of an organisation's devices and network – is very or fairly well

Perceived importance of advanced technical skills

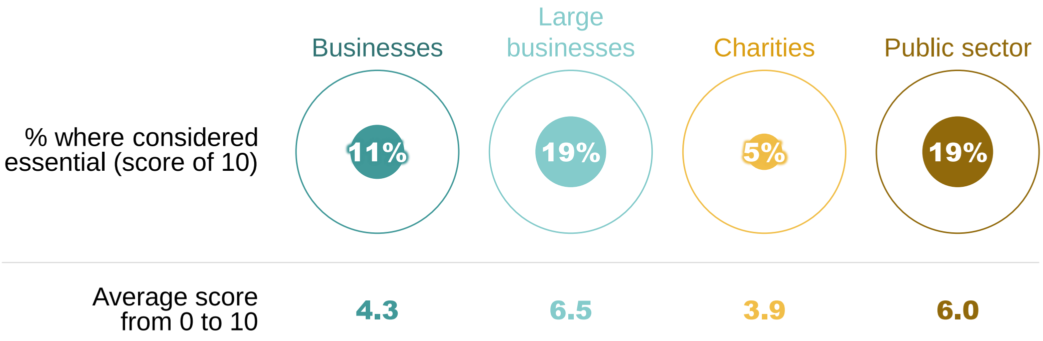
All organisations require basic cyber security skills that allow them to implement basic cyber hygiene measures. Beyond this, some organisations may judge themselves to require more advanced technical skills, based on their perceived level of risk.

Our definition of advanced technical skills came about through the 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 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 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.

[7] 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.

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



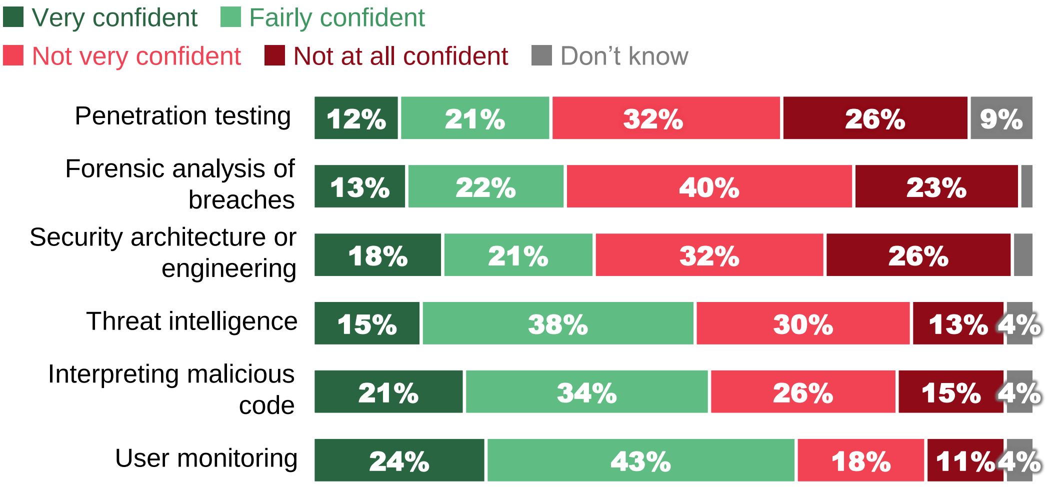
Bases: 947 businesses; 107 large businesses (with 250+ staff); 211 charities; 123 public sector organisations

These advanced technical skills are considered to be more important among the information and communications sector (25%, vs. 11% overall), which is also consistent with previous years.

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[8] and do not outsource these areas of cyber security – i.e. in the cases where businesses have self-identified that they need these types of skills in-house. It suggests that advanced skills gaps are most prevalent when it comes to penetration testing, forensic analysis of breaches and security architecture or engineering. These results echo the 2021 and 2020 findings, in which these 6 skills areas were also ranked in the same order.

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.420+ businesses that do not outsource each task
Unlabelled bars are under 3%.

In Figure 4.5, we rebase these findings out of all businesses (including those that either outsource these tasks or do not consider them as important). This again gives a fuller picture of the proportion of the total

[8] 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).

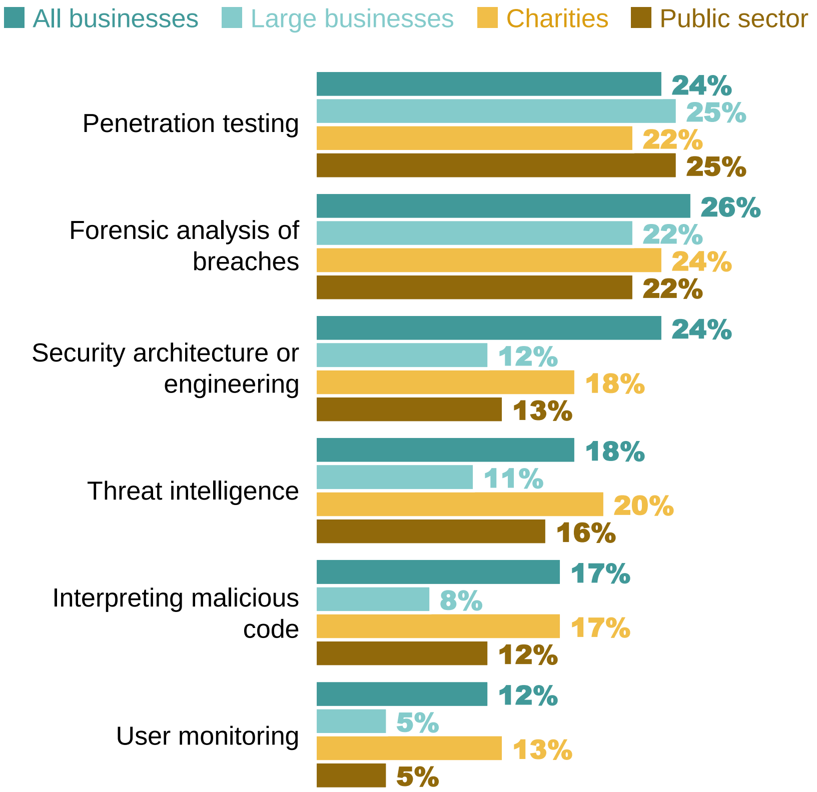
population that has these advanced skills gaps. It also compares this to large businesses and public sector organisations. There are too few charities sampled at this question to be reported here.

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, where organisations do not consider these advanced areas to be important for them, 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 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 penetration testing and forensic analysis – tend to be similarly prevalent across different types of organisations, even different sized organisations. These findings are broadly in line with previous years.

Figure 4.5: Percentage not confident in performing advanced cyber security tasks, by type of organisation



Bases: 947 businesses; 107 large businesses (with 250+ staff); 123 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 and public sector organisations (c.60+).

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 328,000 businesses (24%) have a skills gap in penetration testing
- Around 355,000 (26%) have a skills gap in forensic analysis

- Around 328,000 (24%) have a skills gap in security architecture
- Around 246,000 (18%) have a skills gap in threat intelligence
- Around 232,000 (17%) have a skills gap in interpreting malicious code
- Around 164,000 (12%) have a skills gap in user activity monitoring

A combined advanced technical skills gap indicator

Just as we do for the basic cyber security skills gap calculation, we have merged the 6 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.

By this measure, a third of businesses (33%) have an advanced technical skills gap which equates to approximately 451,000 UK businesses. Around 3 in 10 charities (29%) and a third of public sector organisations (36%) also have an advanced skills gap.

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 2022. They are reported here for the first time. The survey methodologies used in both the sectoral analysis and this cyber security skills study are the same.

Around a fifth of cyber sector employers (20%) report having existing employees who lack necessary technical skills. Just 3 per cent of employers specifically say this prevents them meeting their business goals to a *great* extent, while 17 per cent say it does so to *some* extent.

By contrast, more than double this number of cyber firms (45%) say that the job applicants they have seen lack necessary technical skills. In total, 19 per cent say this is to a great extent, while 25 per cent say it is to some extent.

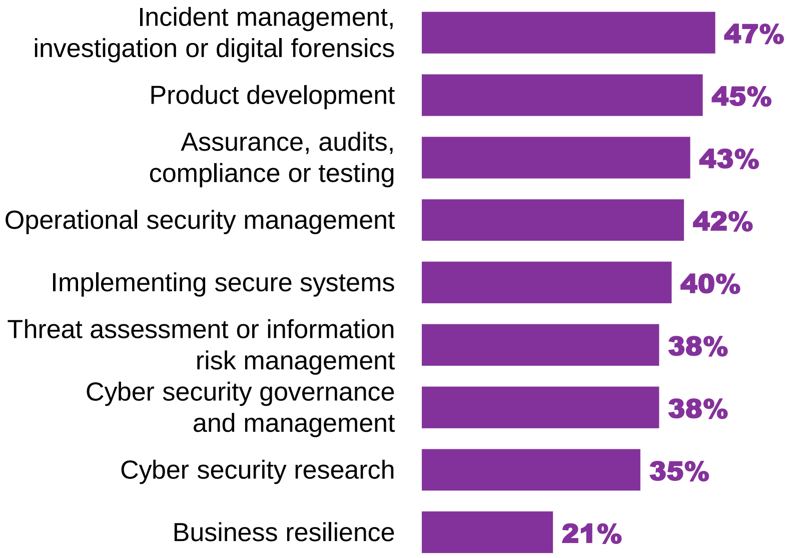
Both these figures remain lower than in the 2020 survey, and more in line with last year's results. The technical skills gap measure is 12 percentage points lower for existing employees than in 2020 (when it was 32%) and 14 percentage points lower for job applicants than in 2020 (when it was 59%). In 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 around half of cyber firms (49%) 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 closer to the 2021 result (47%).

Among this 49 per cent 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. For the first time this year, we added a new category on product development, which registers as one of the top areas for skills gaps in the chart.

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: 122 cyber sector businesses identifying any skills gaps

In summary, there is still an overall shortfall of a wide range of specific skillsets. Skills gaps tend to be, relatively speaking, equally prevalent in a range of areas like incident management, investigation or digital forensics, through to cyber security governance and management. They tend to be less prevalent for business resilience.

Compared to the 2021 results, there are higher skills gaps in the following areas:

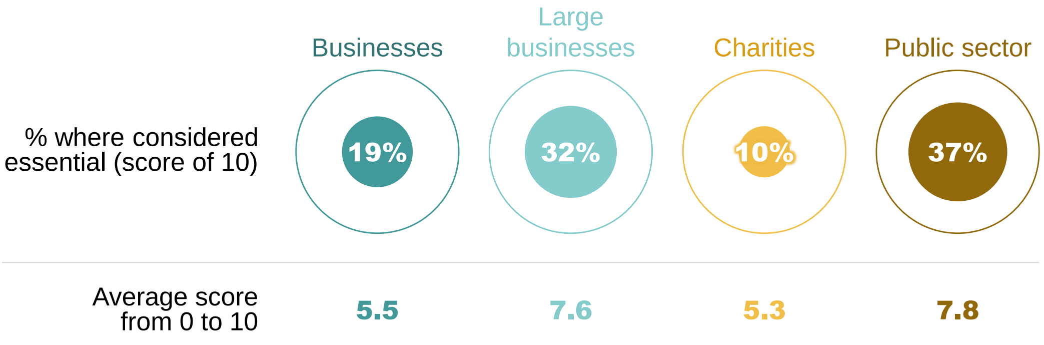
- Operational security management (42% vs. 21% in 2021)
- Implementing secure systems (40%, vs. 22% in 2021) – this has returned nearer to the 2020 level (42%)

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 just a fifth (19%) of businesses consider these skills to be essential, rising to nearly a third of large businesses and around two-fifths of the public sector. This is similar to previous years.

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



Bases: 947 businesses; 107 large businesses (with 250+ staff); 211 charities; 123 public sector organisations

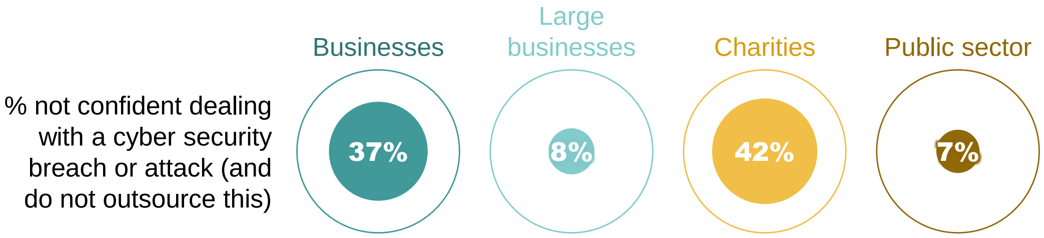
The incident response skills gap

Incident response is still a challenging area for organisations. It is one of the top areas covered by external providers – of the 32 per cent of businesses that outsource any aspect of cyber security, 78 per cent get their external cyber security provider to deal with incident response and recovery.

Among those that do not outsource this function, half of businesses (50%) 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 37 per cent of all UK businesses (when rebased to include those who outsource it) – shown in Figure 4.8.

The all-business figure has risen across the previous 2 years (from 27% in 2020, to 32% in 2021 and 37% now), highlighting an increasing skills gap in incident response and recovery. The change from last year is partly driven by a drop in the outsourcing of incident response and recovery, especially in smaller businesses (see Chapter 9), meaning more firms are now relying on their in-house skills in this area.

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



Bases: 947 businesses; 107 large businesses (with 250+ staff); 211 charities; 123 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+).

This year, there are no statistically significant differences by sector on this measure.

Half of all businesses (49%) are also not confident in their ability to write an incident response plan. A similar proportion of charities (55%) also say this, while the proportion in public sector organisations is lower (23%). There are too few large businesses in the sample to report for this question.

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 soft skills, where a score of 0 means not at all important, and 10 means it is essential. The average result, similar to the 2020 and 2021 scores[9], is 8.4 out of 10. Almost two-fifths (37%) 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 DCMS Cyber Security Sectoral Analysis 2022 (which used a comparable methodology). They are reported here for the first time.

Around 1 in 4 cyber firms (26%) 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 7 per cent say this has stopped them meeting their business goals to a great extent while 19 per cent say this is to some extent. The 26 per cent result is up from 2021 (when it was 18%), reverting closer to the level seen in 2020 (29%).[10]

Around a quarter (28%) say that their existing employees lack these complementary skills (with 3% saying this impacts them to a great extent and 25% 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, the result is that 41 per cent of cyber sector employers have experienced a complementary skills gap in the previous 12 months. This marks an increase in the complementary skills gap (from 31% last year).

Comparing this to the results on technical skills gaps in Section 4.3 (where 49% say they have experienced technical skills gaps) suggests that a lack of complementary skills is almost, but not quite, as big an issue for cyber sector businesses as the lack of technical skills.

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 have skills gaps in these areas.

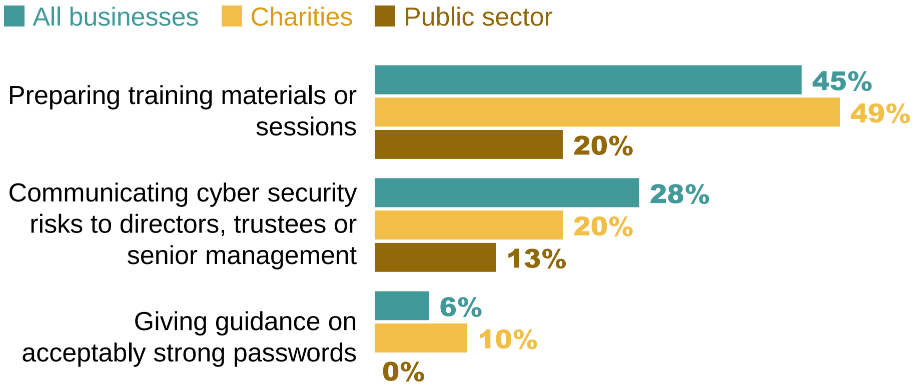
This highlights that preparing cyber security training for staff is something that does not come naturally to many organisations. Chapter 5 highlights how many organisations have actually offered cyber security training to their wider staff, and of these how many have developed any of this training internally.

The results here are similar to previous years.

[9] This year's question changed the phrase "soft skills" to "complementary skills" but the description of what this entailed remained the same.

[10] This year's question wording included "sales and marketing skills" for the first time, which may have served to slightly increase the proportion reporting a complementary skills gap. Therefore, while the question remains broadly comparable, this trend over time needs to be revalidated in later years.

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



Bases (asked to a random half of full sample): c.470 businesses; c.100 charities; c.60 public sector organisations

Qualitative reflections on complementary skills

In the qualitative research, 3 sets of complementary skills were commonly mentioned:

- Communication skills were, in line with previous years, raised as skills gaps within the cyber sector, specifically for sales and client facing roles. Outside the cyber sector, the ability to communicate with impact to senior managers, service providers and other suppliers, and to drive change within an organisation was also considered important. One cyber lead from a local authority noted that the move to virtual interactions under the COVID-19 pandemic had made it harder for their team to network with other local authorities, which is where they would typically build these sorts of skills

- The ability to write well was mentioned in various cyber sector interviews. This was both in terms of technical report writing, once again to distil complex messages for senior audiences, and bid writing to help win new client contracts. One interviewee said this was also an area where there was currently no good training available

- There was also a recurring challenge around being able to persuade non-cyber staff (outside the cyber sector) to follow cyber security policies – the skills to influence behaviour. We touch on this theme again in Chapter 5

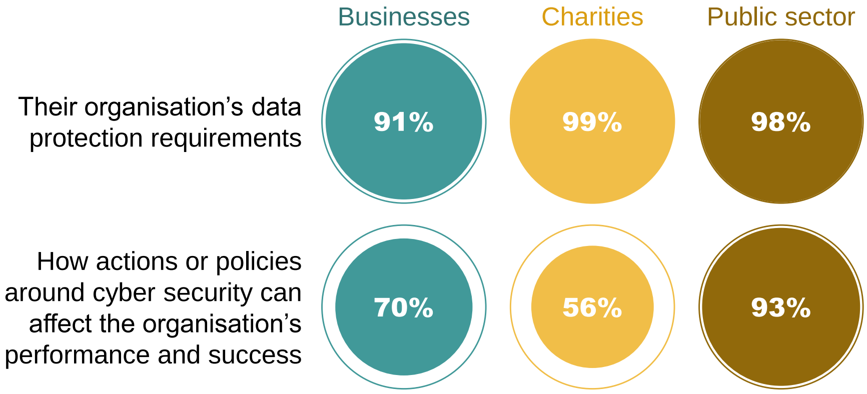
4.5 Governance and compliance skills

Those in cyber roles frequently need strategic management skills to perform their role effectively, particularly in governance, risk and compliance (GRC) roles. The cyber leads in most organisations do not consider themselves to have knowledge gaps in this area, as Figure 4.10 shows. There is a higher level of understanding amongst businesses (91%) and charities (99%) about the organisation's data protection requirements. At the same time, the cyber leads in around 3 in 10 businesses and 4 in 10 charities admit to being uncertain about how cyber security could affect business performance.

The strongest contrast between these two results is with charities. This might indicate the framing of cyber security in these organisations, with a heavier emphasis on data protection than on other aspects of cyber security. This has been evidenced in previous iterations of the DCMS Cyber Security Breaches Survey, for example.

These results are consistent with previous years.

Figure 4.10: Percentage that feel they understand the following aspects of cyber security strategic management very or fairly well



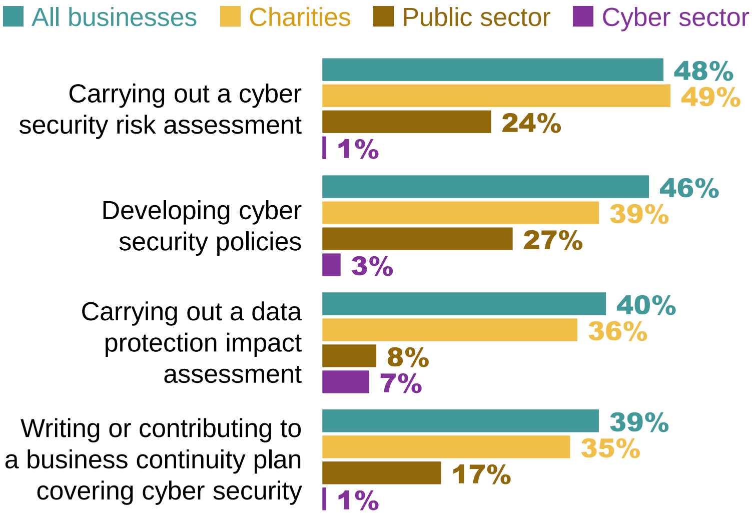
Bases (asked to a random half of full sample): c.470 businesses; c.100 charities; c.60 public sector organisations

When it comes to people in cyber roles being able to carry out cyber security governance tasks, there are widespread self-identified skills gaps. As Figure 4.11 suggests, almost half of private sector cyber leads are not confident in their ability to carry out a cyber security risk assessment or developing cyber security policies. Around 4 in 10 also lack confidence in carrying out data protection impact assessments or 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 under 10% saying they are not confident in each area).

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

Figure 4.11: Percentage not confident in carrying out a range of cyber security governance tasks



Bases (asked to a random half of full sample): c.470 businesses; c.100 charities; c.60 public sector organisations; c.110 cyber sector businesses

Elsewhere in the survey, we establish the perceived importance of this broader GRC knowledge among cyber sector employers. Around 4 in 10 (41%) say it is essential for their staff to have an understanding of the legal or compliance issues affecting cyber security. This is lower than in 2021 (when it was 51%) but still indicates a widespread demand for staff to have this sort of GRC knowledge.

4.6 Cyber security skills gaps in the non-cyber workforce

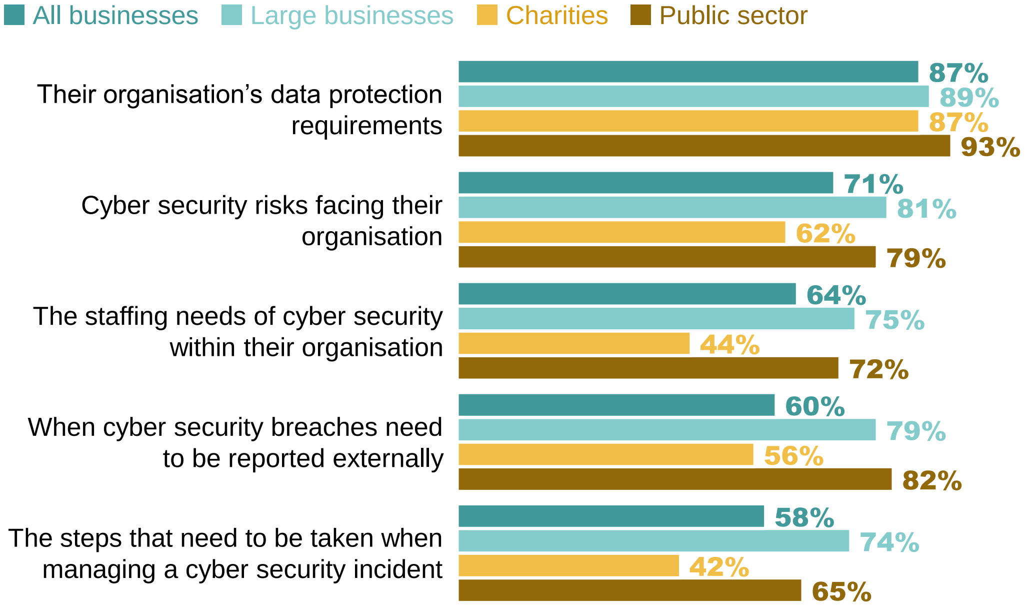
Senior managers and wider staff outside of cyber teams also needed to have the right skills and knowledge to be able to understand and interpret cyber risks, recognise their GRC responsibilities, and follow the cyber security rules and processes set by their organisation. This section explores skills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

Cyber security skills at the board level

Figure 4.12 shows the mixed perceptions that cyber leads outside the cyber sector have of their management boards. In the private sector, for example, around 4 in 10 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. Approximately 3 in 10 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 and staffing 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 4.12: Percentage of cyber team heads that feel their organisation's senior managers understand the following aspects of cyber security very or fairly well



Bases: 947 businesses; 107 large businesses (with 250+ staff); 211 charities; 123 public sector organisations

Across these indicators, cyber leads in the finance and insurance sector, information and communications sector, and education sector (a mix of private and public) tend to have a more favourable opinion of their senior management, whereas those in the food and hospitality sector tend to be less favourable than usual. For example, 9 in 10 in finance and insurance firms (90%, vs. an average of 60%), 8 in 10 information and communications firms (83%) and three-quarters of the education sector (74%) say their senior management understand their cyber security incident reporting requirements, while just two-fifths of those in food and hospitality businesses (37%) say this.

The importance of technical skills and knowledge in board decision making

In last year's report, a major qualitative theme was the perceived lack of understanding of cyber security within management boards (outside the cyber sector), particularly from a technical perspective. This was also a recurring theme in this year's qualitative interviews. Whilst the survey data shows that boards are, by large, attuned to data protection requirements and the cyber security risks facing their organisation, the qualitative findings suggest there is often still a disconnect between the decision making around IT infrastructure and cyber security at the board level, and the technical expertise within IT or cyber teams.

"Because we've moved online, I know there's a push from our Chief Executive to use our IT suppliers less, because we don't need them to be checking our servers. But I don't think they appreciate that, just because something's online, it's going to work or that it's safe."
Organisation outside the cyber sector

This year's interviews highlight a potential knowledge deficit among c-suite decision makers who are tasked with overseeing cyber security, such as Chief Technology Officers (CTOs), Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs). As noted in Chapter 2, people in these roles could often lack a generalist knowledge of cyber security, having come to the role through different specialisms and with widely varying experience. The findings suggest the absence of a comprehensive generalist training pathway for individuals moving into these positions, alongside other challenges such as a lack of time to dedicate to cyber security.

"Cyber isn't fully understood by most businesses. The problem is you have CTOs and CIOs making decisions, but they don't necessarily have the security understanding."
Recruitment agent

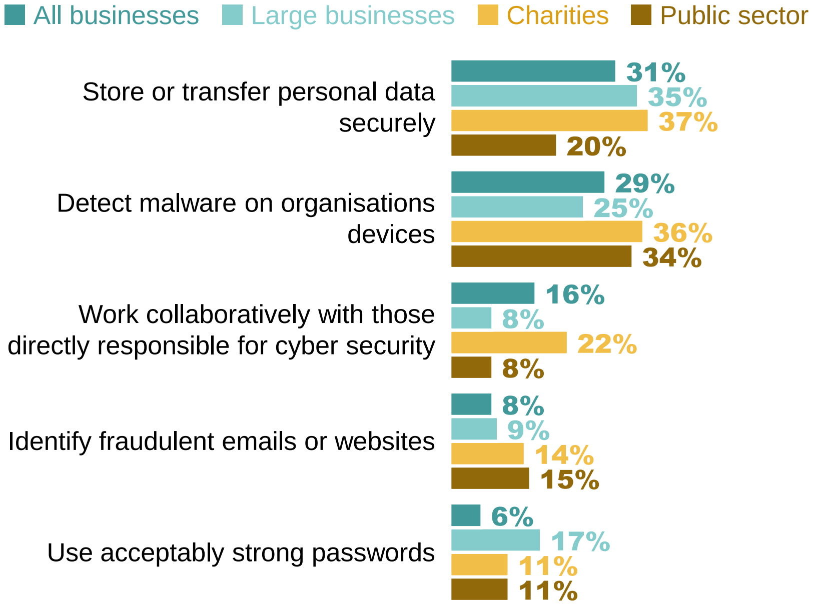
Cyber security skills among wider staff

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

Figure 4.13 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 leads have are around staff not being able to store and transfer personal data securely and not detecting malware on their devices. This is consistent across all types of organisations, with no discernible difference between larger and smaller businesses. Moreover, in large businesses, there is more scepticism about staff using acceptably strong passwords than in the typical business (17% not confident, vs. 6% across all businesses).

These results are, again, in line 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 (65% confident now, vs. 58% in 2018).

Figure 4.13: Percentage not confident in non-specialist staff being able to carry out various tasks that can impact on cyber security



Bases: 947 businesses; 107 large businesses (with 250+ staff); 211 charities; 123 public sector organisations

Across several of these indicators, those in information and communications businesses, and finance and insurance businesses again tend to be more confident than average about their wider staff acting appropriately when it comes to cyber security. In addition, specifically on personal data handling, cyber leads in the health and social care sector (a mix of public and private) also tend to rate their staff highly (77% are confident in their staff in this regard, vs. a 65% average across the public and private sectors).

5 Training and upskilling

This chapter explores organisations' cyber security training needs, the types of training undertaken and how effective it is seen to be. It covers training for those in cyber roles and for wider non-specialist staff.

Key findings

- Half of all cyber sector businesses (51%) have undertaken a cyber security training needs analysis in the past year. Less than a fifth of other businesses (17%) have done so
- Three-quarters (73%) of cyber sector firms have provided training to staff in cyber roles this year, compared to a fifth (21%) of other private sector businesses
- More cyber sector firms are providing training for career starters than last year (59% of the firms providing any training, vs. 45% in 2021) a return to the level seen in the 2020 study
- Just 1 in 9 businesses (11%) have provided cyber security training to non-cyber staff

5.1 Training needs

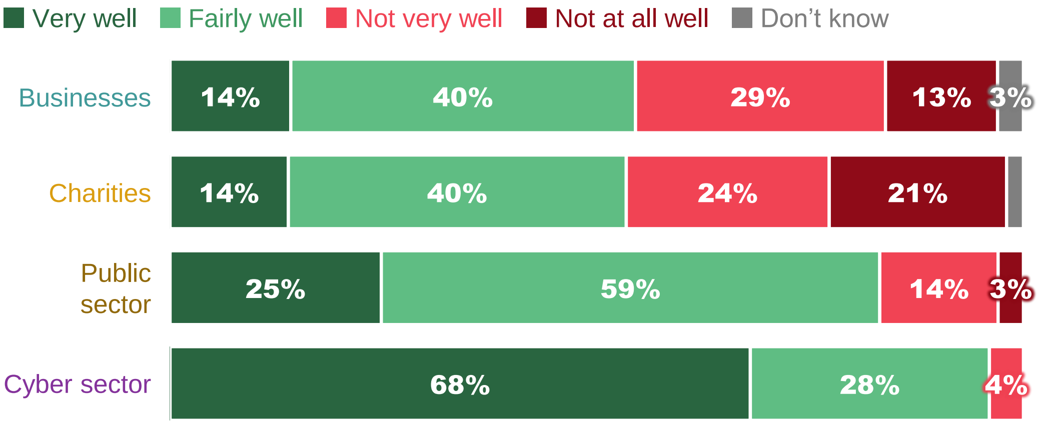
How well organisations feel they understand their training needs

Most organisations feel they understand their cyber security training needs at least fairly well – more than half of all businesses (54%) say this – but few outside the cyber sector say they understand these needs *very* well, as Figure 5.1 shows. While this result is lower than last year (when it was 62%), there is no consistent trend upwards or downwards across the previous studies.

Like in previous years, public sector organisations tend to report that they understand their training needs better than businesses and charities (83% at least fairly well).

In the case of cyber sector businesses, more than two-thirds (68%) feel they understand their training needs very well. As in the 2020 and 2021 surveys, this still leaves around a third that do not pick this top answer, suggesting there is still room for development.

Figure 5.1: Extent to which organisations feel they understand their cyber security training needs



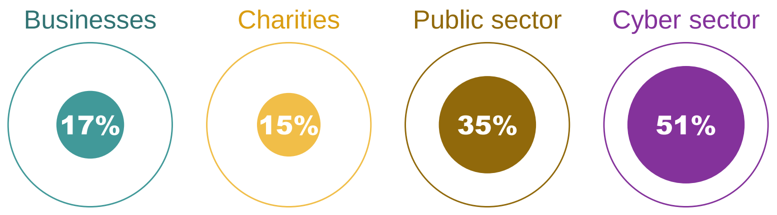
Bases: 947 businesses; 211 charities; 123 public sector organisations; 224 cyber sector businesses
Unlabelled bars are under 3%.

Information and communications businesses are more likely than average to say they understand their cyber security training needs *very* well (33%, vs. 14% overall). Large businesses also tend to report a better understanding of their training needs, with 3 in 10 (28%) saying they understand them very well, and 8 in 10 (83%, vs. 54% overall) saying they understand them at least fairly well. These differences were also present in the 2021 study.

Formally analysing training needs

The self-reported understanding of training needs amongst organisations can be contrasted against the proportion that have undertaken a formal training needs analysis. As Figure 5.2 shows, less than a fifth of businesses and charities have done this within the past year. Cyber training needs analyses are more common in the cyber sector, as might be expected, and public sector. This is all, broadly, consistent with previous years' results – there is no clear upwards or downwards trend across years.

Figure 5.2: Percentage of organisations that have undertaken a formal analysis of cyber security training needs in the last 12 months



Bases: 947 businesses; 211 charities; 123 public sector organisations; 224 cyber sector businesses

The following subgroups are more likely than average to have undertaken such an analysis, reflecting their relatively high engagement with cyber security generally:

- Finance and insurance firms (43%, vs. 17% overall)
- Information and communications firms (42%)
- Medium businesses (36%)
- Large businesses (35%)

5.2 Training undertaken by those in cyber roles

One business in five (21%) report having any of their staff in cyber roles undertake training relevant to their roles in the last year. The proportion is slightly higher for charities (27%) and substantially higher among public sector organisations (56%). As might be expected, cyber sector firms report the highest amount of training undertaken (73%) among their cyber professionals.

The cyber sector finding has fluctuated across years, albeit within the margins of error – and with no consistent trend. For the remaining groups, these results are in line with those from 2021.

Businesses in the finance and insurance sector (51%, vs. 21% overall) and information and communications sector (46%) are more likely than average to have had cyber security staff undertaking training. It is also far more likely for medium (50%) and large businesses (65%) to provide such training than the average business. These differences are also consistent with last year's findings.

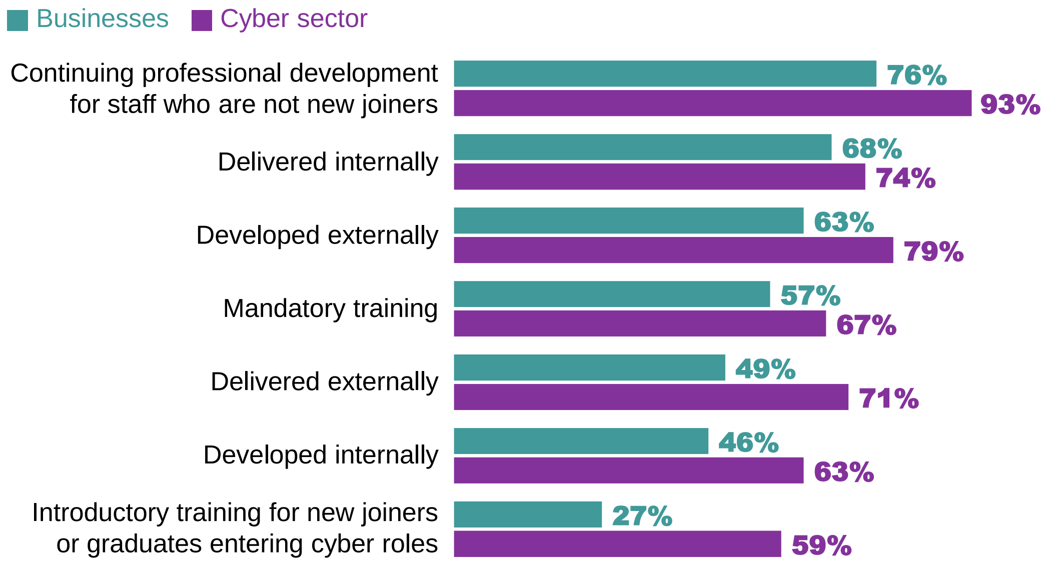
Features of the training being undertaken

Figure 5.3 shows the nature of this training, among the firms that provide it. We only show findings for non-cyber businesses and for cyber sector firms.

This training continues to be more directed at established cyber security staff rather than career starters in these roles, both within and outside the cyber sector. However, more cyber sector firms are providing training for career starters this year (up from 45% in 2021 to 59% now, among those where any cyber staff are undertaking training). This year's result is more in line with the 2020 report (when it was 63%), suggesting that this is not a consistent upwards trend. Nevertheless, it supports the trend evidenced in Chapter 2, suggesting that more businesses in the sector are taking on career starters than before.

Organisations providing training for those in cyber roles often draw on a mix of external and internal sources. Training is more likely to be *developed* externally than in-house but is more likely to be *delivered* internally than externally across the private sector – a pattern continued from previous years. In the cyber sector specifically, training tends to be delivered internally and externally in equal measure.

Figure 5.3: Percentage of organisations where staff in cyber roles have undertaken the following type of training in the last 12 months, among the organisations that have provided training to this group



Bases (among those that have had staff in cyber roles undertake training): 335 businesses; 163 cyber firms

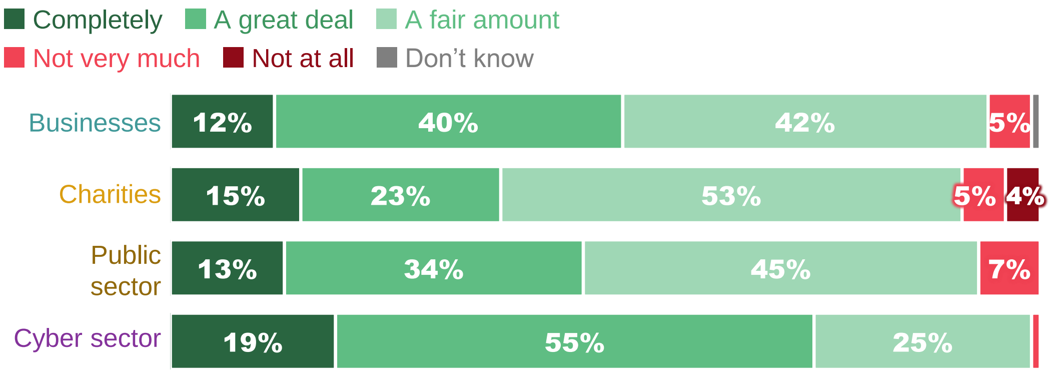
The pattern of findings for charities and public sector organisations is similar to businesses, but the filtered samples for these groups are relatively small at this question, so they have not been included in the chart. One notable difference is that public sector organisations are more likely than private sector ones to have had training developed externally for their cyber staff (81%, vs. 63% of businesses).

Perceived effectiveness of training for those in cyber roles

Figure 5.4 shows that the cyber sector businesses that have invested in training for those in cyber roles are, on balance, positive about the effectiveness of this training (74% say the training met at least *a great deal* of their needs). However, there is less confidence outside the cyber sector in this kind of training being fit for purpose (this is 52% in the wider business population where training is provided).

The proportion of businesses (of those providing training) saying the needs of their cyber staff were met *completely* has fallen this year (to 12%, vs. 20% in 2021 and 19% in 2020).

Figure 5.4: Extent to which organisations feel that the training for those in cyber roles met their needs (where such training has been undertaken)



Bases (among organisations that have had staff in cyber roles undertake training): 335 businesses; 70 public sector organisations; 82 charities; 163 cyber sector businesses
Unlabelled bars are under 3%.

Time and administrative barriers to training for those in cyber roles

In the qualitative interviews, a common barrier to training for cyber teams was the time investment required. Attending training was felt to take people away from billable work or other core responsibilities. This was an issue within and outside the cyber sector. Some interviewees said it had been exacerbated by the COVID-19 pandemic. For example, one cyber lead outside the cyber sector said they had paused their Certified Information Systems Security Professional (CISSP) training during the pandemic because of the pressure on their team to carry out core IT responsibilities.

A lack of time and human resources functions were also considered as barriers to training others. One cyber firm said that it would take around 4 to 5 years for them to train entry-level staff, and they currently did not have the capacity among senior staff to provide supervision or training for this time period. Another noted that they would need to scale up their human resources and management capabilities before they could take on entry-level staff such as apprentices. One idea, from a different interviewee outside the cyber sector, was to have a network of people from similar sectors that had run successful cyber apprenticeship schemes, so that organisations could discuss challenges and share best practice.

The organisations that had provided training to junior staff (at all levels, not just entry level) often built time for this into their business models. One described training and mentoring of junior staff as one of the highlights of the job for many of their team. And, as we discuss further in Chapter 6, the training offer was often a selling point for organisations when it came to recruitment into cyber roles.

Qualitative reflections on different training approaches for those in cyber roles

In the qualitative research, we found employers often using a mix of 5 different styles of training. These were a mix of on-the-job and off-the-job training approaches:

- Some larger cyber sector businesses offered an academy model, where staff receive ongoing training and development over a longer time period, typically several months. One large firm had a scheme, which was open to people with and without cyber backgrounds through a 2-year programme of online training and formal rotations through different cyber teams. The idea was to identify which technical team the individual would fit best in, while also giving them a grounding in all aspects of cyber security, so they could cross-sell to clients.

- There continued to be a large emphasis on self-guided training, as seen in previous years – this is where staff took it on themselves to pursue courses that were largely online. This was considered less of a time burden than face-to-face training. Some cyber sector employers had purchased licences or credits with external online training platforms such as the Knowledge Academy and Coursera. This kind of training was often gamified – one cyber firm, for example, hosted a chat group for their staff to compete over how many courses they had completed.

  There were, however, challenges associated with online training generally. A common theme was that online training courses often lacked depth – something we discuss further in Section 5.4

- Work shadowing was used to train people on-the-job. This approach was also raised in previous years as a way of informally training staff within the constraints of a smaller business. However, one cyber lead pointed out that shadowing was not possible for some cyber security roles that are time-critical, such as incident response and recovery, because it slowed down the teams at work

- An important theme this year was mentoring – assigning more senior staff to be mentors to junior staff, to help them build their confidence and applied knowledge over a longer time period. In the experience of one cyber training firm, private sector clients often undervalued the importance of mentoring and had initially sought cheaper, short-term training solutions before turning to them. In one instance, they had moved a company from relying on basic online courses, which staff were not completing, to a 9-month mentoring programme, which recognised that different staff had arrived at their roles with different backgrounds and skillsets in cyber security

- Internal knowledge sharing was considered an important way to get the maximum value from any training or research activity. One cyber sector employer had a very structured process for this. They had twice-weekly sessions where a senior and junior engineer would write code to achieve an objective, then compare their work. They also had an employee in a cyber security research role, who ran monthly sessions around new innovations and attack vectors in cyber security. Finally, they ran monthly lunch-and-learn sessions where anyone who had attended a formal training course would relay what they had learnt to the rest of the company. This was also a way of quality-assuring the training (see Section 5.5)

Approaches to Continuing Professional Development

In the qualitative interviews, the idea of Continuing Professional Development (CPD) in cyber roles was generally given more attention in cyber firms than outside the cyber sector. Those that had a CISSP qualification had to continue training each year to maintain this. Some businesses identified the training needed for career progression in appraisals and personal development plans. Nevertheless, some cyber said they were still too small or newly established to have career development pathways for their staff.

A common challenge was that cyber staff often had very diverse career backgrounds and, in roles like security engineering, a very broad set of training pathways that they could follow. This meant that CPD often consisted of very bespoke discussions between individuals and line managers, and there was little uniformity across staff. For instance, one large cyber firm had split their cyber staff into 12 specialisms and mapped the competencies required in each one. However, they said 80 per cent of the pathway to meet these competencies was about learning from colleagues, rather than structured training.

Outside the cyber sector, there were additional CPD challenges for staff in cyber roles. Often, there was no pressure or emphasis from senior managers on CPD. In some cases, it was implicitly discouraged, as senior managers preferred staff to be dealing with immediate IT issues.

"Cyber security is on my management's radar, but I think they'd rather I was sitting at my desk fixing problems, sorting things out, rather than taking part in a webinar doing my CPD."
Organisation outside the cyber sector

In addition, even where these cyber leads felt empowered to request CPD training, they sometimes lacked a sense of the training they needed. One cyber lead we spoke to was uncertain whether they needed training on penetration testing, for which they had recently been approached by an external provider. This hints at the need for a clear, generalist training pathway. However, as noted in Chapter 2, the generalist pathway in the UK Cyber Security Council's Careers Route Map may have a limited appeal with this group at present, as some do not see themselves as *cyber* professionals.

"Someone like Barclays invites you to a cyber event. You turn up and the National Cyber Security Centre (NCSC) gives you some advice, but they don't tell you: 'why don't you do a course on this'."
Organisation outside the cyber sector

5.3 Attitudes towards the Cyber Security Body Of Knowledge (CyBOK)

The Cyber Security Body Of Knowledge (CyBOK) is a knowledge framework to inform and underpin education and professional training for the cyber security sector. It covers 21 distinct knowledge areas and is maintained by the cyber security community.

In the qualitative interviews, we asked interviewees to review the summary documentation for the 21 knowledge areas before the interviews. CyBOK received mixed views. One employer viewed it as a comprehensive document that they could adapt to introduce their entry-level staff to the breadth of cyber security and all its specialisms. One recruitment agent also noted how it was a helpful resource for them to appear credible when speaking to cyber security hiring managers.

However, other cyber employers and hiring managers felt it was of little use to them directly. Most commonly, they felt that the document was too long and academic for their purposes – some felt it could have been written in plainer English to be more useful in a commercial context.

A specific area of feedback was around CyBOK's integration with international frameworks, like the US government's National Initiative for Cybersecurity Education (NICE) framework. One cyber training provider said that some of their global clients would often have adopted the NICE framework in their training programme, and that CyBOK's usefulness would increase if it was more integrated with this alternative framework.

5.4 Cyber security training or awareness raising activities for wider staff

Overall, 1 in 9 businesses (11%) and 1 in 5 charities (20%) have provided cyber security training to non-cyber employees in the last year. There are substantive differences by size, with this kind of training being much more common in medium (41%) and large businesses (54%). Public sector organisations are also much closer to larger businesses in this regard, with 5 in 10 (52%) having provided cyber security training to this wider group of staff.

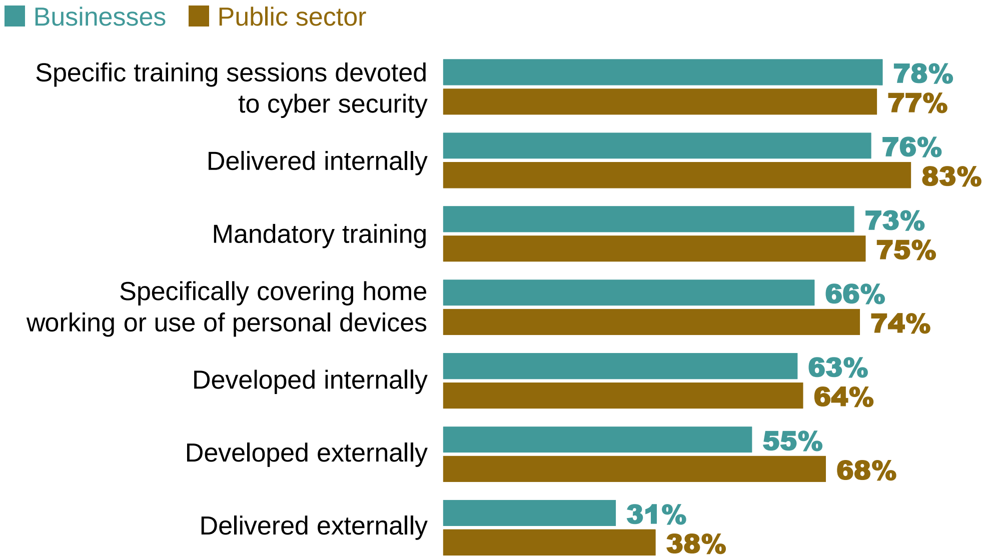
Cyber security training for wider staff is more prevalent in the finance and insurance sector (32%) and information and communications sector (28%). It is especially uncommon in the construction sector (6%) and food and hospitality sector (3%).

These findings (overall and sector subgroups) are very similar to the 2021 and 2020 surveys.

Features of the training being undertaken with wider staff

As Figure 5.5 shows, in the private sector these training sessions are more likely to be both developed and delivered internally rather than externally, in contrast to training for those in cyber roles (where externally developed training content is the norm). In most, but not all cases, they are specific training sessions for cyber security (78%) – the remaining 22 per cent may be, for example, GDPR-related training that touches on cyber security. They are also more likely to be mandatory than training sessions for those in cyber roles (73%, vs. 57% for those in cyber roles in the wider private sector). These patterns are all in line with previous years.

Figure 5.5: Percentage of businesses and public sector organisations where non-specialist staff have attended the following type of cyber security training or awareness raising sessions in the last 12 months, among the organisations that have provided training to this group



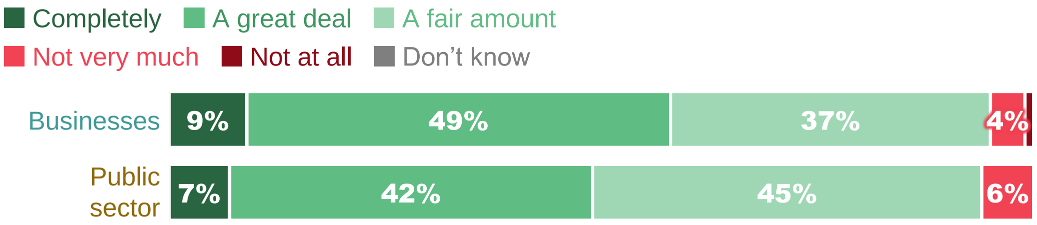
Bases (among those that have undertaken training or awareness raising sessions for non-specialist staff): 230 businesses; 62 public sector organisations

Perceived effectiveness of training for wider staff

Around 3 in 5 businesses (59%) and half of all public sector organisations (49%) think that any cyber security training for wider staff met the needs of the organisation *a great deal* or *completely*. This highlights the ongoing room for improvement in training approaches. The sample size for charities is too low to report this question.

These results are broadly consistent with those from 2021 and 2020.

Figure 5.6: Extent to which businesses and public sector organisations feel that the cyber security training or awareness raising sessions for non-specialist staff met their needs (where such sessions have been administered)



Base: 230 businesses that have undertaken training or awareness raising sessions for non-specialist staff; 62 public sector organisations that have undertaken training or awareness raising sessions for non-specialist staff;

Unlabelled bars are under 3%.

Challenges around training wider staff

The qualitative research raised the following themes around cyber security training for wider staff:

- A key challenge was getting staff to believe they need to do cyber security training. One firm highlighted the need for continuous communication on the topic and mandated training. Another common theme was around needing to be non-technical – and to link cyber security and the implications of cyber security incidents to people's day-to-day behaviour, including outside work

> ***"What we are trying to encourage is to not think of it as technical training but as life training. If you've got a mobile phone, you can get a text which is cyber related just as much as you could get an email that you could click on."***
> *Organisation outside the cyber sector*

- Good training needs to test people's understanding in some way. One public sector organisation noted that this was a positive feature of the NCSC's free training, which includes a quiz at the end

- A one-size-fits-all approach was not necessarily the best one. Some organisations noted the wide variation in understanding and proficiencies around cyber security across their core staff, meaning that an ideal approach would cater to different groups

- One public sector organisation specifically mentioned the need for more training courses catering for management boards – training courses that are short and less detailed than those for IT teams, but still provide an overview of aspects of cyber security that the board needs to understand

- Finally, the move from face-to-face to virtual training under the COVID-19 pandemic continued to have mixed implications. While online delivery may have been less impactful, one cyber lead raised some benefits. They felt staff recognised the need for cyber training more in a hybrid working environment. They also thought a greater proportion of their staff were now exposed to cyber security training, because virtual sessions could be more easily and frequently scheduled

5.5 Identifying high-quality external training

A recurring theme in the qualitative interviews was the existence of low-quality cyber security training in the external training market. Some cyber leads noted that fast-turnaround training courses for those in cyber roles were too focused on getting staff to pass an exam without imparting practical knowledge.

One cyber training provider argued that this was a potential market failure. In their experience, organisations purchased training primarily based on cost and speed, without initially recognising the value of longer-form courses. This had incentivised low-quality training courses to enter the market, which had in turn made it harder for organisations to distinguish good and bad training. The same interviewee felt that colleges and higher education providers had also skewed the market in this direction, by favouring short form, externally delivered courses that had high pass rates. One marker of this was the wide gap in the charges between the cheapest and most expensive training providers.

"In the UK you get offered rates of £250 a day … Why would anybody take that? As a training consultant, £850 is the minimum you could earn in the UK as a day rate, so if you're capable of delivering a course, you should be capable of being a consultant."
Cyber sector business

In this environment, organisations had various approaches to identify high-quality training:

- Outside the cyber sector, there were examples where organisations looked at recommendations from government sources (including the devolved administrations), or from their own IT or cyber security providers

- Within and outside the cyber sector, there was a strong emphasis on staff feedback on training. One cyber firm had senior people go through training courses before other staff, to quality-assure the content. Another had staff specify the intended outputs and outcomes of any external course beforehand, and reassessed whether these had been met in their personal development plans after taking the course. One public sector organisation had carried out a focus group with staff that had tried different training courses

- Also across sectors, there were frequent mentions of the CISSP qualification. As one of the most well-established qualifications in the market, this was seen to give a good generalist grounding in cyber security. It was also, as per previous years, felt to be the most widely recognised qualification among clients, making it attractive to cyber firms

- Finally, one of the cyber firms using online training platforms said they opted to use platforms that had a reputation to maintain, and therefore an incentive to provide good-quality training (they mentioned the Knowledge Academy and AWS Academy)

6 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 2020, encompassing the roughly 18 months prior to the fieldwork for this project. This is to remove any overlap with the timeframe accounted for in the previous survey (the 18 months since the start of January 2019). Therefore, this is the first survey in the series to focus largely on post-pandemic recruitment.

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 7.

Key findings

- More than half of cyber sector businesses (53%) have tried to recruit someone in a cyber role since the beginning of 2020. The average number of vacancies per firm has gone up from 5.2 in the 2021 report to 6.8 this year
- The most common recruitment approaches continue to be using recruitment agents (39% of the firms with vacancies), social networks such as LinkedIn (38%) and word-of-mouth recommendations (29%). Over the last 3 studies there has been a trend away from recruitment agents and more towards social networks for recruitment
- More than four in ten cyber vacancies (44%) posted since the start of 2020 are reported as being hard to fill, which is slightly higher than the estimate from last year (37%) and the year before (35%). The most common reason given for this continues to be around candidates lacking technical skills or knowledge, but mentions of increased competition from other employers have increased since the 2021 report
- 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

6.1 Approaches to recruitment

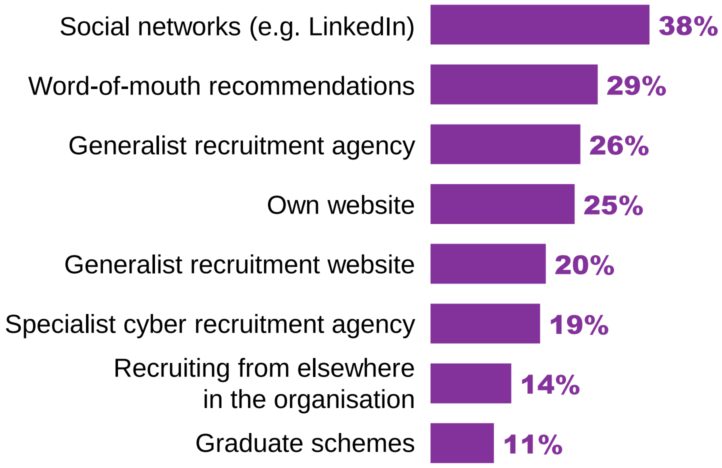
More than half of all cyber sector businesses (53%) have tried to recruit someone in a cyber role since the beginning of 2020. While this is similar to the previous year's result (47%), it is worth noting that the average (mean) number of vacancies per firm has gone up from 5.2 last year to 6.8 this year. Furthermore, the job vacancies analysis covered later (in Chapter 7) highlights that the total number of cyber security vacancies across the economy as a whole (i.e. within and outside the cyber sector) has also dramatically increased.

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

Most common recruitment methods

Figure 6.1 shows the most common recruitment methods used to find candidates for cyber roles, among the 53 per cent of businesses that have posted vacancies. Social networks, word-of-mouth recommendations and recruitment agents (either generalists or specialists) continue to be the most common channels for recruitment.

Figure 6.1: Percentage of cyber firms with vacancies that have used the following recruitment methods (unprompted – multiple answers allowed)



Base: 118 cyber sector businesses that have had vacancies in cyber roles since the start of 2020
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. Two-fifths (37%) of the cyber firms that have had vacancies have used just 1 of the methods mentioned in Figure 6.1 to fill these vacancies. A total of 1 in 3 (30%) have used 2 methods and around a quarter (24%) have used 3 or more methods.

Changes over time in recruitment methods

While recruitment agents are still frequently used, there has been an overall decline in their use as measured across the last 3 studies. Around a quarter each use generalist recruitment agents (26%), while one in five use specialists (19%) which, when combined, equates to 4 in 10 cyber sector employers with vacancies (39%). In the 2021 study, this combined result was 48 per cent, while the 2020 study it was 54 per cent.[11] Specifically, it is the use of specialist recruitment agencies that has gone down from 35 per cent in the 2020 study, to 25 per cent last year, and 19 per cent this year.

By contrast, the reliance on social networks (such as LinkedIn) has increased over the course of the 3 studies in this series. In the 2020 study, it was 26 per cent, rising to 35 per cent in 2021 and 38 per cent in this latest study.

This year's results also provide some indications that cyber firms are both more likely to be recruiting internally (recruitment from elsewhere in the organisation has risen from 6% to 14%) and at junior levels (the use of graduate schemes has risen from 5% to 11%). These particular trends are based on small

[11] The 2020 study looked at recruitment approaches used across the 3 previous years, rather than just 1 year. The 54 per cent result may have been slightly lower if we had only asked about 1 year of recruitment. However, the data still suggests an overall downward trend.

sample sizes and just 2 years of data (given changes to the answer categories between the 2020 and 2021 studies) – they should be considered indicative and need to be validated with further years of data. Nevertheless, these indicative findings broadly support the analysis in Chapter 2 that a wider range of employers are taking on career starters than before.

Qualitative findings on job specifications

A key finding last year was that job specifications were often unrealistic in their demands, tried to recruit multiple roles in one, or were not reflective of the actual requirements for the role on offer. The qualitative research this year indicates that poorly written job specifications continue to be a problem in cyber recruitment. This was felt to be a greater issue with less experienced clients – those recruiting a cyber role for the first time or who had previously only had someone transition into that role from another area, such as IT.

"You only get that from the less mature clients … Most clients have hired before and are willing to take our advice so they will adjust their requirements and not be unrealistic. 30 per cent of clients will be unrealistic in the first instance and then the market talks."

Recruitment agent

One recruitment agent pointed out that for hiring managers, writing a job specification was a relatively small part of their job, meaning it did not always get the level of care and attention it might deserve. In another interview, a hiring manager told us their typical approach was to use other job adverts they found online as their baseline for creating their own job specification.

The same recruitment agent said they commonly saw job specifications that asked for too many skillsets, giving no narrative overview of the kind of individual they were looking for. They generally ignored the spec they had been given, had a conversation with the hiring manager about the role being advertised, and then wrote their own specification to accommodate this role.

The training offer was viewed as a strong selling point in job specifications, and one that was sometimes underappreciated or undersold by employers, according to recruitment agents.

"Cyber people are like the military – they love to train."

Cyber sector business

6.2 Assessing candidate aptitude

The qualitative interviews reveal 3 common approaches to assessing candidate aptitude:

- Employers often made a highly qualitative initial assessment of job applicants, often drawing more conclusions from a simple conversation with candidates than by looking at their qualifications or career backgrounds. Qualifications were still a means to sift candidates for interviewing (for non-entry level roles) but not a guarantee that candidates were job-ready

  "I know within 10 minutes of talking to them … If they start talking about cyber security risk as opposed to information risk, there are little indicators that they don't know what they are talking about."

  Cyber sector business

- Alongside this broader qualitative assessment, there was a very strong emphasis across the board on formally testing technical knowledge and skills in some form during the recruitment process. These were commonly bespoke tests or scenarios designed by the hiring manager to reflect their business needs. Often, hiring managers were not simply looking at whether candidates had passed or failed, but more broadly whether they had demonstrated the right qualities in going about the test or exercise – for instance, aptitude to learn and tenacity. In a couple of cases, employers had given candidates open book exercises, where they could go away and research the problem before coming back with an answer

- Complementing the survey findings, word-of-mouth recommendations continued to be very important for both employers and recruitment agents. This was not only to find potential job candidates but also to validate the skills of those that had applied. One cyber sector employer said that, upon receiving a CV, he would call around other cyber firms to check their reputation

> ***"Within 30 minutes, I've got a background check on that individual in terms of whether they are who they say they are in terms of their capabilities.***
> *Cyber sector business*

In terms of the overall balance of approaches used, we found that some employers tended to lean more on word-of-mouth and their own qualitative assessment, while some focused more on formal tests.

6.3 Hard-to-fill vacancies and skills shortages

Among the 53 per cent of cyber sector firms that have had any cyber security vacancies since the start of 2020, almost 7 in 10 (67%) had at least one vacancy that they considered to be hard to fill. This is higher than the result recorded in the 2 previous studies (57% in both previous years).

When taken as a proportion of all cyber sector employers (i.e. including those that have not recruited in the last 18 months), this equates to 35 per cent of all cyber employers saying they have had at least one hard-to-fill vacancy.

From another perspective, we estimate that almost half (44%) of all the *vacancies* posted since the start of 2020 are hard-to-fill vacancies, which is slightly higher than the estimate from last year (37%) and the year before (35%). This is indicative evidence that the cyber security skills shortage has increased, amid dramatically rising demand for candidates to fill cyber roles (which we cover in Chapter 7). More years of data would be required to properly validate this trend.

For added context, the 2019 Employer Skills Survey showed that 23 per cent of all digital sector vacancies in the UK were deemed hard-to-fill. This provides an indication of the greater scale of this issue in the cyber sector.[12]

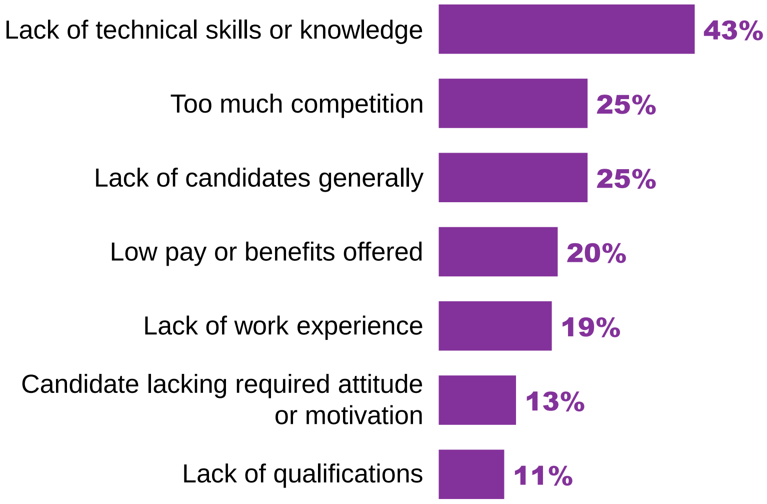
Reasons behind hard-to-fill vacancies

As Figure 6.2 shows, among the 35 per cent 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 2021 and 2020 studies.

[12] This is the most recently available data from the Employer Skills Survey as of the publication of this report, with fieldwork carried out before the COVID-19 pandemic. The Employer Skills Survey is a telephone survey weighted to be representative of UK business establishments, although this statistic excludes Scotland data. It calculates hard-to-fill vacancies using a comparable methodology to our survey, but does so at an establishment level (i.e. including branch offices) rather than an enterprise level, which may lead to different findings.

The proportion highlighting competition from other employers was relatively consistent in both previous studies (10% in 2020 and 9% in 2021). This year, it is among the most common spontaneous reasons offered for vacancies being hard to fill (25%). It should be remembered that these figures reflect a subset (35%) of all cyber sector firms. Nevertheless, among this subset, this again reflects the substantial increase in demand this year for cyber security staff. It links to the wider theme from the qualitative interviews (covered more in Chapter 8) that this is a candidate-driven market at present.

Figure 6.2: Most common reasons offered by cyber sector businesses for having hard-to-fill vacancies (unprompted – multiple answers allowed)



Base: 79 cyber sector businesses that have had hard-to-fill vacancies in cyber roles since the start of 2020
Only specific categories mentioned by 10% or more shown.

For context, the latest DCMS Cyber Security Sectoral Analysis provides supporting evidence that competition between cyber sector employers for new talent has increased. It finds that the total size of the workforce in the cyber sector has increased by approximately 6,000 full-time equivalent (FTE) employees. However, this is within a tighter labour market, where a greater number of employers are competing for staff from the cyber security recruitment pool. This is explored further in Chapter 10, which estimates the size of the annual workforce gap.

Specific roles most affected by skills shortages

The survey findings suggest that there are a mix of skills shortages across both generalist and specialist cyber roles, in roughly equal measure. For the specialist categories (Figure 6.4), this year's results are not directly comparable to previous years. We adopted an updated list of job roles that better reflected DCMS's categorisation, and which aligned to the work of the UK Cyber Security Council and the CyBOK.

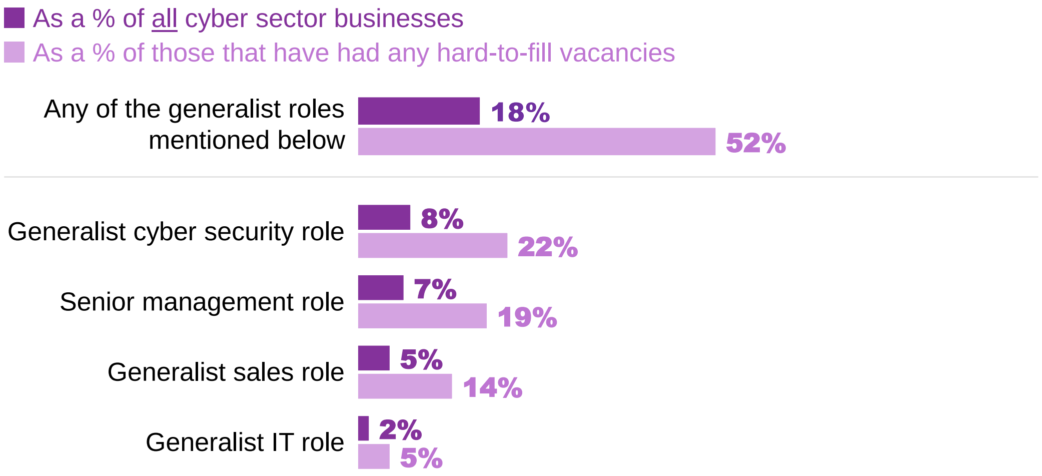
Among the cyber sector businesses that have had hard-to-fill vacancies, around half (52%) say they have had such vacancies in generalist roles (Figure 6.3). This amounts to around 1 in 5 cyber sector firms (18%) across the overall sector population. These results are in line with last year.[13]

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

[13] In last year's findings 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. Therefore, the 18 per cent and 52 per cent results at Figure 6.3 are not directly comparable to last year's equivalent chart. Given the regrouping, these results are in line with last year.

executive board) as well as IT and sales roles that require cyber security knowledge or involve cyber security functions.

Figure 6.3: Percentage of cyber sector firms that have found it hard to fill the following generalist job roles (multiple answers allowed)

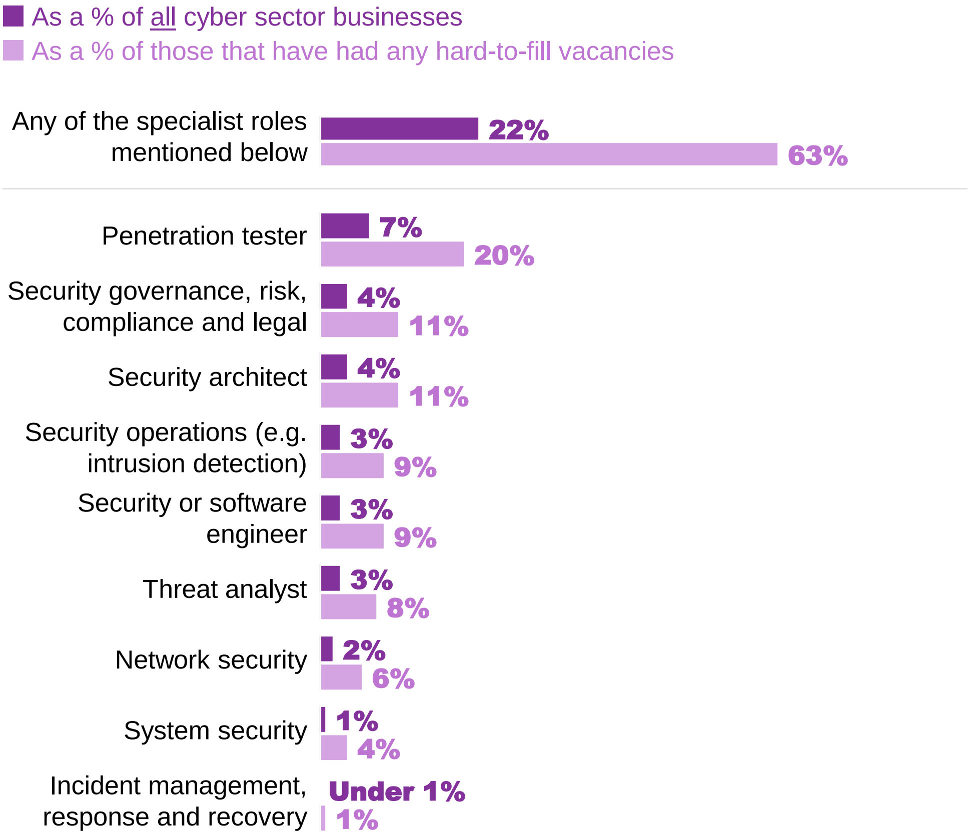


Bases: 224 cyber sector businesses; 79 that have had hard-to-fill vacancies in cyber roles since the start of 2020

Among those that have had hard-to-fill vacancies, 6 in 10 (63%) have had such vacancies in specialist roles. This equates to a fifth (22%) of all cyber sector firms. Figure 6.4 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.

While penetration testing features at the top of this list by a small margin, it is one of the least common job roles being advertised across the labour market (see Chapter 7). Therefore, this appears to be a niche skillset that is hard to come by, for the relatively small number of firms that require it.

Figure 6.4: Percentage of cyber sector firms that have found it hard to fill the following specialist job roles (multiple answers allowed)



Bases: 224 cyber sector businesses; 79 that have had hard-to-fill vacancies in cyber roles since the start of 2020

Qualitative evidence on hard-to-fill roles

It should be noted that, as the later findings in Chapter 7 show, there is an increased demand for people to fill all sorts of cyber roles. Bearing this in mind, the qualitative research suggests that certain roles have more persistent shortages. The following roles were commonly mentioned (across multiple interviews) and have all been mentioned in previous years as well:

- Cloud security roles – an area where demand was felt to have substantially increased as a result of the pandemic, with more organisations moving to the cloud
- DevSecOps
- Security architecture

The following roles were mentioned by individual employers or recruiters as particularly difficult to recruit:

- Application security – one recruiter noted that the skillset for this role heavily overlapped with architecture and development roles, which were more attractive to candidates

> ***"Specialised security roles require lots of fire-fighting and enormous challenges. I think people have heard of this and tend to err on something that is maybe safer or less of a leap."***
> *Recruitment agent*

- Generalist cyber security roles with expertise in small and medium enterprises

- Roles working for Critical National Infrastructure (CNI) – one recruiter highlighted that CNI organisations often had bespoke technology and 24-hour servicing, making it harder for individuals in cyber roles to transfer to and across CNI organisations

> ***"You can't just take someone from Barclays and put them in that same role in BP."***
> *Recruitment agent*

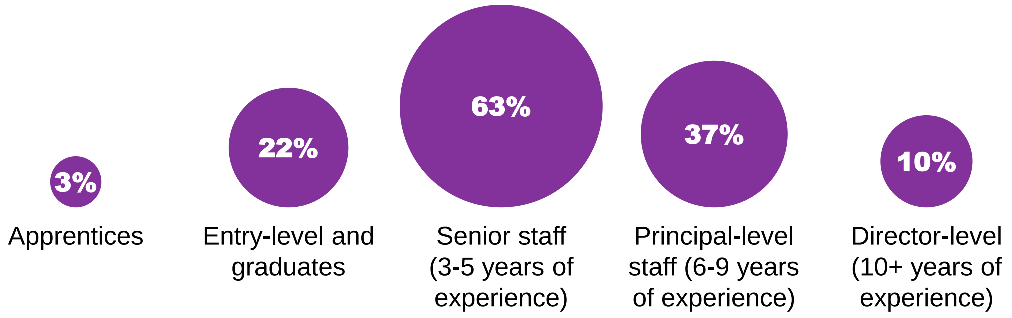
- Network security specialists
- Operational resilience roles – this has been in response to the Prudential Regulation Authority's operational resilience policy, which comes into effect from the end of March 2022 for a wide range of finance and insurance firms
- Security engineering (with a specific mention of Security Operations Centre, or SOC engineers)

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 6.5). These findings are in line with the 2021 results. This continues to broadly match the findings from the job vacancies analysis (see Chapter 7). That analysis shows that around half of all vacancies are set at the 3 to 5 years of experience range, so it makes sense that this would be where the bulk 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. Almost 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 per cent of all job postings in the latest data (in Chapter 7). In other words, these higher-level jobs are hard to fill, for reasons beyond intense demand.

Figure 6.5: 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 2020

The qualitative interviews highlight a particular issue for organisations with older systems when recruiting entry-level and mid-level staff in cyber roles. One public sector organisation felt that people with a long career ahead of them in cyber security would be less interested in dealing with legacy systems like theirs. The hiring manager felt that their job specification, which focused on maintaining current systems, did not present an attractive offer, since the skills gained by someone in the role would be less transferrable.

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

The impact of hard-to-fill vacancies varied. In the qualitative interviews, there were examples of these vacancies leading to more pressure on existing staff to fill the gaps or bringing external contractors in for this purpose. There were also examples from recruiters of where organisations had increased the salary on offer, changed the job specification to allow home working or added their training proposition.

Recruitment agents said that a common approach for them when faced with hard-to-fill roles was to speak directly to hiring managers rather than to human resources (HR) staff, to help them revise their job specification. One recruiter reported that, with generalist cyber roles outside the cyber sector, this conversation would often help to clarify the true balance of technical skills versus governance, risk and compliance (GRC) skills required for the role.

However, a challenge recruiters faced was the limited feedback they tended to get from organisations. The potential barriers raised by HR staff is covered in the next section.

"Many clients don't want to be specific, as it allows us to push back, I think."

Recruitment agent

6.4 The role of human resources (HR) in recruitment

In the qualitative research, the larger organisations we spoke to had HR support functions. However, the qualitative interviews indicate that there is sometimes a lack of awareness about the role of HR in recruitment among cyber security hiring managers. While some hiring managers understood that their HR colleagues were involved in sifting applications, they had no knowledge of the approaches taken.

In our interviews, there were cases where HR was a positive force in broadening out the methods of recruitment used. In one public sector organisation, HR colleagues had been the driving force for the organisation to look at apprenticeships in the IT team, and more generally they were closely involved in reviewing job specifications, benchmarking salaries and talking to recruiters.

At the same time, recruitment agents mentioned their experiences of HR staff sometimes acting as a block on recruitment. There was a sense that relationships between recruitment agents and HR tended to be less personal and more transactional, compared to agents and hiring managers. They felt that HR staff were often more process-driven and less focused on outcomes for hiring managers. There was also a perception that HR staff are, by their nature, generalists who do not understand the differences between cyber roles. One recruiter noted various experiences where HR staff had not allowed them to speak directly to the hiring manager, leading the recruiter to turn down the contract with the organisation.

7 Cyber security job vacancies

This chapter sets out a profile of online cyber security job vacancies, based on our analysis of the secondary job data through the Burning Glass Technologies labour market database. It covers 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 being offered. The data focuses on the 2021 calendar year (1 January to 31 December).

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. There are often very subtle differences in the data, for example between regions (Figure 7.3). For this reason, we report some of the findings in this chapter to 1 decimal place, to show these subtle variations more accurately.

We complement the secondary data on salaries with the qualitative findings on this topic as well.

Key findings

- The demand for cyber security professionals has increased significantly in 2021. On average, there were 4,400 core cyber security postings each month. This is an increase of 58 per cent compared to 2020 levels
- There is emerging 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)
- Employers continue to place an emphasis on recruiting those with at 3 to 5 years of experience
- Across the 12 months of 2021, the average (mean) advertised salary was £60,100 for a core cyber job posting (with a median of £55,000). This reflects a nominal mean increase of £900 (+1.5%) and nominal median increase of £2,000 (+3.7%) from 2020 levels

7.1 Core versus cyber enabled job roles

The separately published technical report comprehensively lays out the methodology used for this analysis. An important aspect to bear in mind when reading this chapter is that, just as in the 2020 and 2021 reports, we split cyber job roles into *core* and *cyber-enabled* job roles.

- 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

- Cyber-enabled roles are not formally 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 both core and cyber-enabled job roles typically require a mix of technical and non-technical cyber security skills. Therefore, these cannot simply be differentiated as technical vs. non-technical jobs in cyber security.

To be clear, this is a different distinction from the formal versus informal cyber roles discussed in Chapter 4, 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.

7.2 Number of job postings

Figure 7.1 shows the monthly trend for a period of 24 months from January 2020. This covers the months prior to the initial COVID-19 lockdown in the UK (in March 2020) and up to the end of 2021.

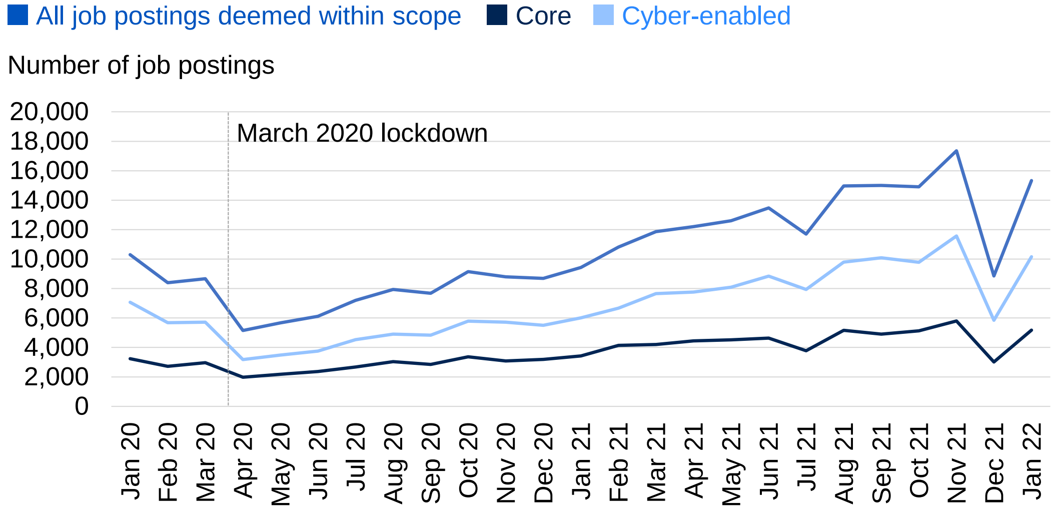
Whilst there was a significant drop in the number of cyber security job vacancies in quarter 2 of 2020, the labour market showed swift signs of recovery, with demand recovering to pre-pandemic levels by autumn 2020. The subsequent data for 2021 shows a continuous and substantial upwards trend.

Between January 2021 and December 2021, there were 153,192 cyber security job postings, including:

- 53,144 core cyber roles (an average of 4,429 per month)
- 100,048 cyber-enabled roles (an average of 8,337 per month)

This compares to 33,622 core cyber roles and 60,125 cyber-enabled roles across 2020. In other words, the core cyber job postings have increased by 58 per cent, and the cyber-enabled job postings have increased by 66 per cent from 2020 to 2021. The drop in postings between November and December 2021 is likely to be a seasonal drop and is not indicative of this broader trend – this is evident from the immediate return to the broader trend in January 2022 (added to the next 2 charts for context).

Figure 7.1: Monthly number of core and cyber-enabled online job postings from January 2020 to December 2021

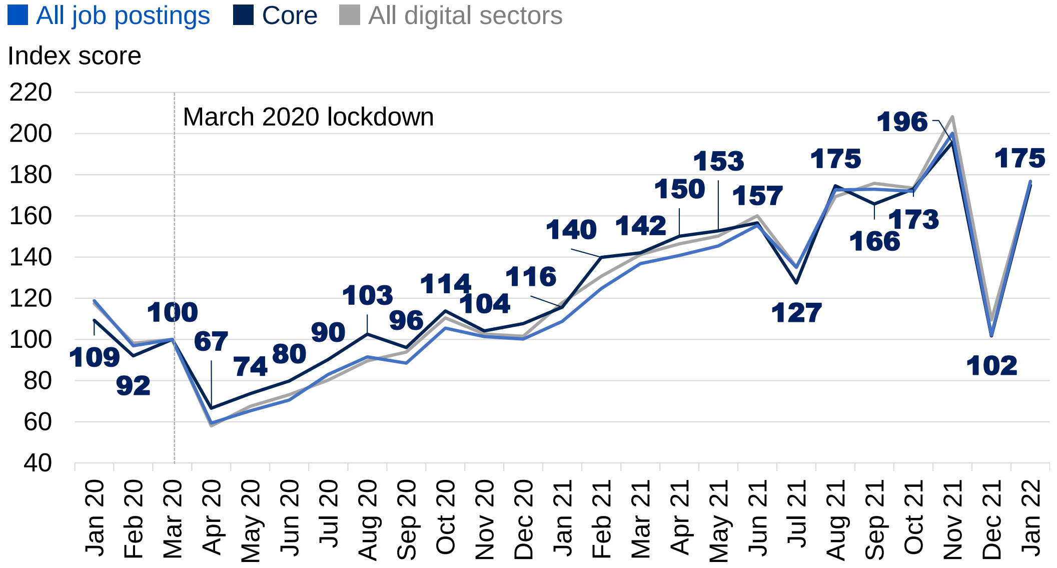


Source: Burning Glass Technologies
Bases: 262,275 online job postings from January 2020 to January 2022 (of which 153,192 were in 2021); 91,943 core (53,144 in 2021); 170,332 cyber-enabled (100,048 in 2021)

Figure 7.2 demonstrates how the volume of cyber security job postings has changed since March 2020 (i.e. the first COVID-19 lockdown). The job postings for all other months are indexed to this month, which has a score of 100. In other words, the score for each subsequent month shows the per cent change in vacancies compared to March 2020.

This chart shows that cyber security online job postings had recovered to consistent pre-pandemic levels by October 2020. The 2021 data suggests a significant further month-on-month growth in demand for cyber security talent. The month of July 2021 was an outlier in the face of this overall trend. We have included January 2022 in this chart because of the suspected seasonal drop highlighted in Figure 7.1.

Figure 7.2: Index of online job postings (March 2020 = 100)



Source: Burning Glass Technologies
Bases: 262,275 online job postings from January 2020 to January 2022 (of which 153,192 were in 2021); 91,943 core (53,144 in 2021); 1,924,922 across all digital sectors (1,133,618 in 2021)

In the early stages of the pandemic, as Figure 7.2 indicates, the cyber security labour market grew more rapidly than other digital sectors. Across 2021, the trend was more in line with the wider digital sectors.[14]

7.3 Geographic differences

The rest of this chapter focuses on the online job postings from January 2021 to December 2021, i.e. for a 12-month period.

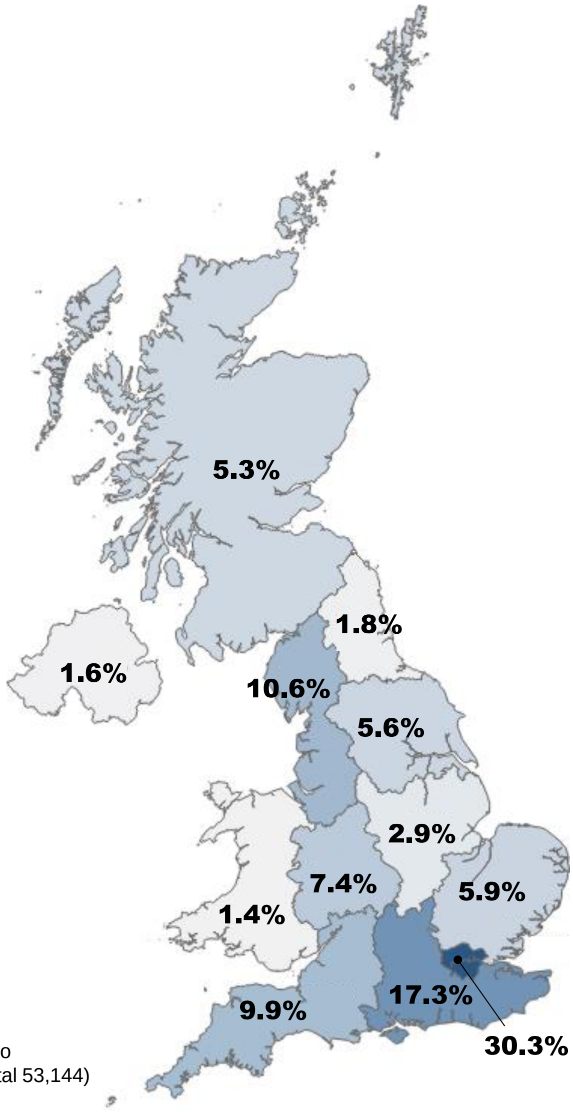
Figure 7.3 shows the proportion of job postings for core cyber roles from each UK region (where the region is known) for 2021. The darker the colour on the heatmap, the higher the density of cyber jobs in that region. This shows, as expected, a clustering of job posts in London and the South East.

However, the percentage of roles in Greater London has fallen proportionately within the last 12 months (from 33.2 per cent of roles to 30.3 per cent) of roles. Furthermore, we estimate that a fifth of roles in 2021 (21%, vs. 13% in 2020) were either UK-wide or remote (and therefore not attributable to a single region). This marks an increased trend towards working from home across all regions in cyber security.

Figure 7.3: Percentage of core cyber job postings from each UK region

Ranking

1. Greater London (30.3%)
2. South East (17.3%)
3. North West (10.6%)
4. South West (9.9%)
5. West Midlands (7.4%)
6. East of England (5.9%)
7. Yorkshire and the Humber (5.6%)
8. Scotland (5.3%)
9. East Midlands (2.9%)
10. Northern Ireland (1.6%)
11. Wales (1.4%)
12. North East (1.8%)



Source: Burning Glass Technologies
Base: 41,803 core cyber job postings from January to December 2021 where region was listed (out of a total 53,144)
Map created using OpenStreetMap data in Mapbox

[14] This reflects the DCMS definition of the digital sectors, covered in the DCMS Sectors Economics Estimates Methodology.

The regional differences in Figure 7.3 are also very broad. They mask the fact that there are strong clusters of cyber security activity within regions. For example, the DCMS Cyber Security Sectoral Analysis has consistently shown particularly strong sector hotspots across the UK's regions. This regional activity was a key consideration in the recent DCMS investment in the UK Cyber Cluster Collaboration (UKC3) initiative.

As with previous years, we have, therefore, carried out more granular geographic analysis using the Travel to Work Areas (TTWAs)[15] in the UK. Figure 7.4 shows the top 15 TTWAs for core cyber job postings in absolute terms and in terms of Location Quotients. The latter measure shows how concentrated labour market demand is within a geographic area. The average demand is set at 1.0. A Location Quotient of 1.2, for example, indicates that the demand for core cyber employees is 20 per cent higher than the UK average. We again illustrate this as a heatmap, with darker blues indicating a higher Location Quotient. Greyed out TTWAs are places where there were a negligible number of job postings in our data (with a Location Quotient that rounds down to 0), or none at all.

[15] For an explanation of TTWAs, see the ONS website. There are a total of 228 TTWAs. The Isle of Man and the Channel Islands are not TTWAs so are not included. Our Location Quotient calculations are based on 2016 Annual Population Survey (APS) data, and the TTWA calculations are based on the April 2011 TTWAs.

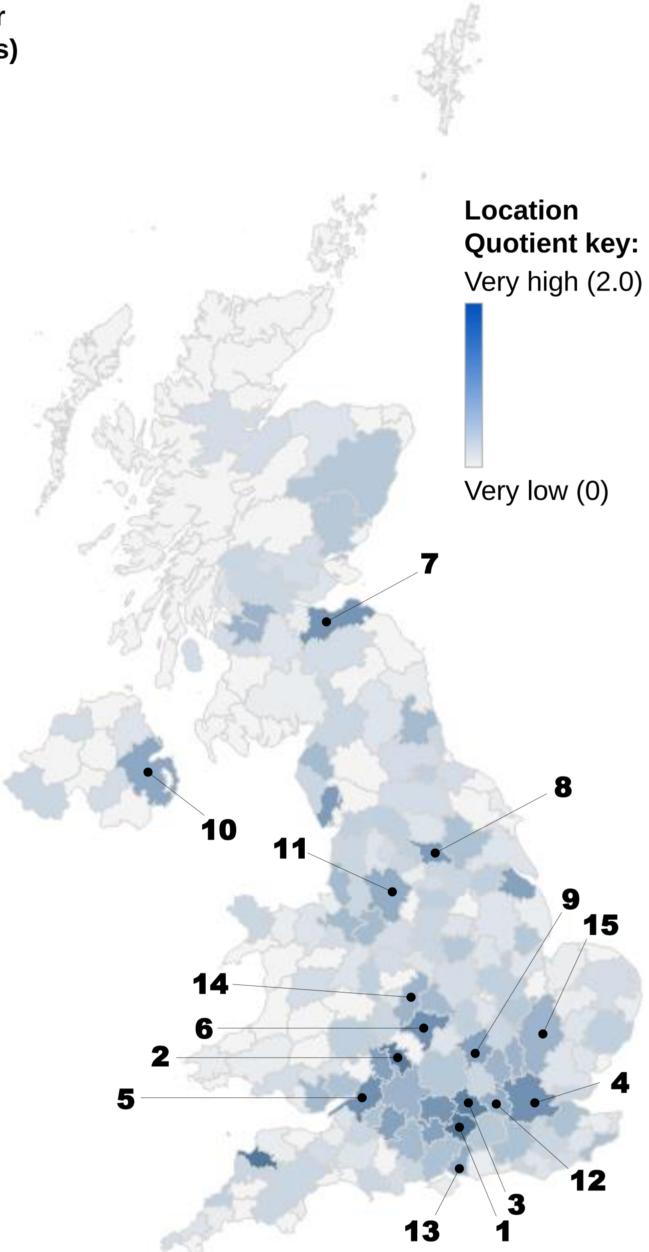
Figure 7.4: Number of core cyber job postings and Location Quotients in the top 15 UK Travel to Work Areas

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

i.	Greater London (12,238)
ii.	Manchester (2,047)
iii.	Bristol (1,493)
iv.	Birmingham (1,201)
v.	Leeds (1,037)
vi.	Edinburgh (965)
vii.	Reading (894)
viii.	Cambridge (703)
ix.	Glasgow (703)
x.	Belfast (624)
xi.	Guildford and Aldershot (479)
xii.	Liverpool (461)
xiii.	Slough and Heathrow (439)
xiv.	Nottingham (398)
xv.	Luton (344)

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

1.	Basingstoke (2.0)
2.	Cheltenham (1.9)
3.	Reading (1.8)
4.	Greater London (1.5)
5.	Bristol (1.5)
6.	Leamington Spa (1.5)
7.	Edinburgh (1.4)
8.	Leeds (1.3)
9.	Milton Keynes (1.2)
10.	Belfast (1.1)
11.	Manchester (1.0)
12.	Slough and Heathrow (1.0)
13.	Portsmouth (1.0)
14.	Birmingham (0.9)
15.	Cambridge (0.9)



Source: Burning Glass Technologies
Base: 33,040 core cyber job postings from January to December 2021 where TTWA was listed (out of a total 53,144)
Map created using OpenStreetMap data in Mapbox. LQ Rank assumes minimum of 200 posts in a region to reduce rank outliers (for small towns). The Isle of Man and the Channel Islands are not TTWAs so are not included.

Looking across both these maps (Figures 7.3 and 7.4) highlights specific areas, or hotspots, where there is both a high absolute number of core cyber job postings and where they make up a relatively high proportion of the local economy.

These hotspots continue, in line with previous years, to include London and other cities like Leeds, Edinburgh, and Belfast. The analysis also highlights the continued strong demand for core cyber jobs across the West Midlands and the South West (in Bristol, Cheltenham, and wider Gloucestershire).

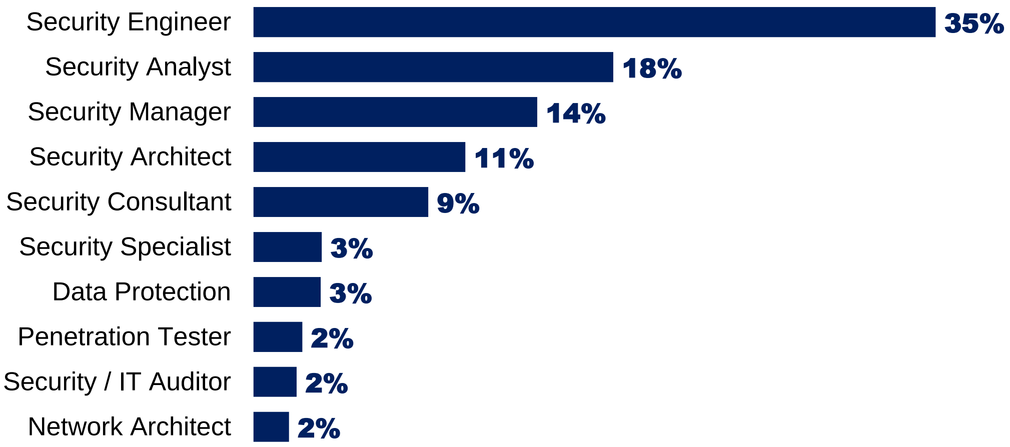
As a caveat to this geographic analysis, both Figures 7.3 and 7.4 may slightly underestimate the extent of cyber security labour market activity in certain regions. In locations such as Wales and the East Midlands, there are a small number of very large firms that dominate the local cyber security labour market. For example, DCMS's Cyber Security Sectoral Analysis 2022 found that 4 per cent of office locations in the cyber sector are in the East Midlands and a further 3 per cent are in Wales, but neither register a high number of cyber security job postings in our labour market analysis. These larger firms often have a wider range of recruitment approaches and may not always post job adverts online. The Burning Glass Technologies dataset only accounts for online job postings, so may therefore underrepresent these types of employers.

In an appendix at the end of this report, we bring together the regional findings from across this chapter, to illustrate the current state of the cyber security labour market in each region.

7.4 The job roles being advertised

Figure 7.5 lists the identified core cyber roles by job title. In our analysis, minor variations (e.g. Security Engineer and Cyber Security Engineer) have been combined.[16] These figures are consistent with the previous skills studies, suggesting a sustained demand across these roles. Security engineering roles continue to be most in demand by a considerable margin.

Figure 7.5: Top recurring job titles among the core cyber job roles identified



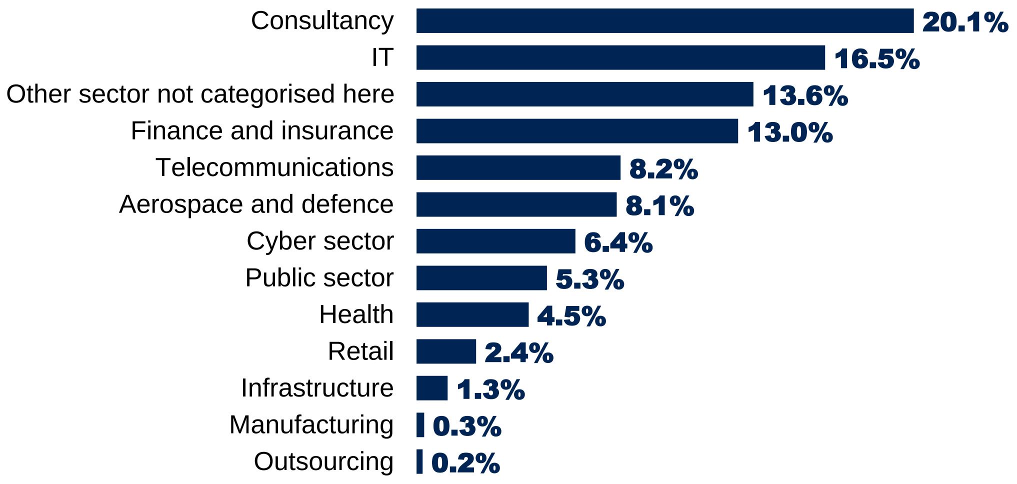
Source: Burning Glass Technologies
Base: 22,550 core cyber job postings from January to December 2021 featuring one of the top 200 job titles (across 53,144 core cyber job postings)

[16] We have focused, within the confines of the analysis possible on the Burning Glass database, on the top 200 job titles appearing in the data. This covers 22,550 of the total 53,144 core job postings for the latest 12-month period. This means some of the very specific variants (e.g. "Security Manager – Banking") may have been missed. However, we expect these to be distributed in the same way as the captured data. Therefore, Figure 7.5 is still expected to be representative of all online job postings in these core roles.

7.5 The sectors demanding cyber security staff

Job postings within the Burning Glass Technologies dataset are typically advertised through a recruitment agency. This means that the employer's name – the end client of the recruitment agency – may not be contained within the job posting. Nevertheless, for the core cyber roles, a total of 8,426 job postings for the latest 12 months (around 16 per cent of all the core cyber job posts identified) have a known employer name[17] and we have categorised these by their sector in Figure 7.6.

Figure 7.6: Percentage of job adverts for core cyber roles coming from specific sectors (where the employer is named)



Source: Burning Glass Technologies; employer data coded by Perspective Economics
Base: 8,426 core cyber job postings from January to December 2021 that have a named employer
Percentages are shown to 1 decimal place to highlight the distinction between the lower ranking responses.

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

Nevertheless, taken at face value, the analysis lines up with other subgroup analysis in this survey and other DCMS surveys on cyber security, and with the data highlighted in previous waves. It suggests that the sectors most in demand of cyber talent are the finance and insurance, information and communications, and professional services sectors.

Of note, compared to the previous year's findings, a higher share of online cyber job vacancies are now in the consultancy (up 2.4 percentage points) and IT sectors (up 2.9 percentage points). Public sector recruitment also makes up a greater share of the market now (up 1.3 percentage points) By contrast, the share taken by the cyber sector has dropped from last year (by 3.5 percentage points). It is of note that some of the UK's leading cyber sector firms have a relatively low volume of job postings in the latest data. This trend ties in with the survey findings in Chapter 6 – these suggest that more cyber sector firms have moved away from direct recruitment approaches (e.g. through large recruitment agents) and increasingly adopted more bespoke methods, such as hunting down individuals through LinkedIn.

[17] This is sourced from an export of the largest 200 companies. We have manually excluded cases where recruitment agencies made the job posting on behalf of another employer.

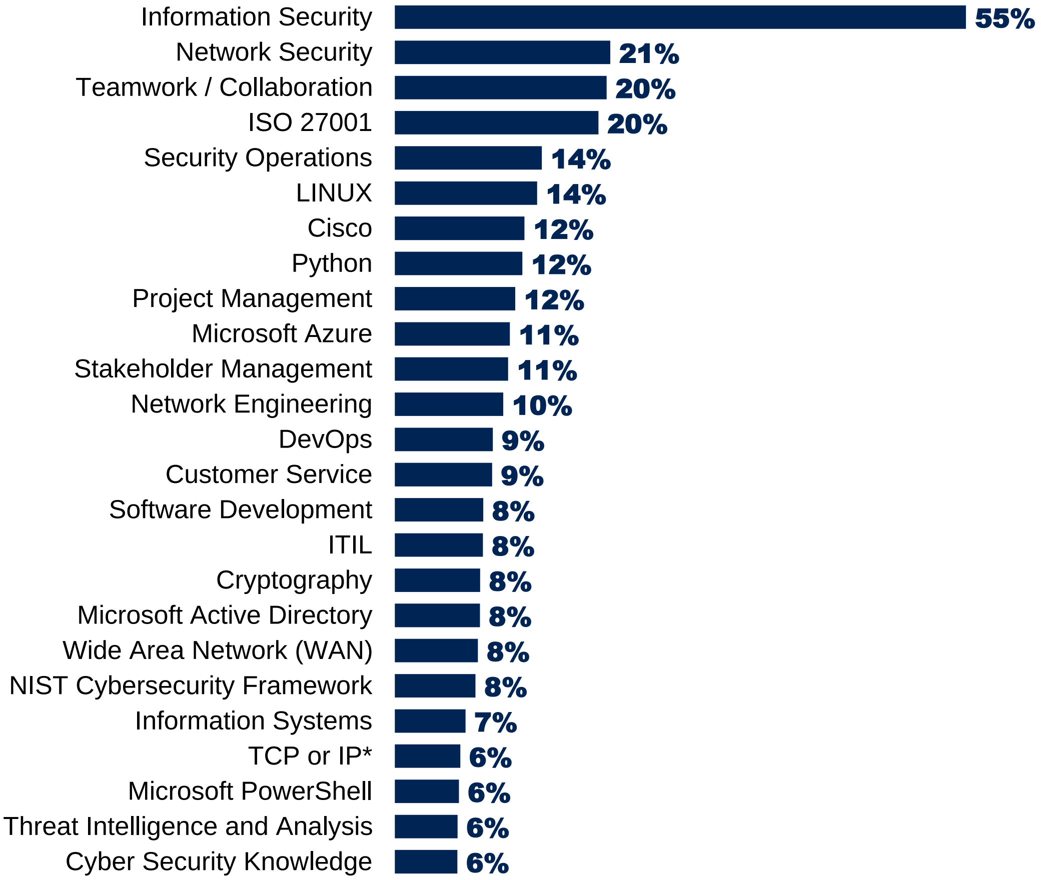
7.6 The skills, qualifications and experience being demanded

This analysis is based on text analytics of the descriptions given for each job posting.

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 the same as in previous years, namely information security skills, network security skills and skills around ISO 27001 (the international information security standard). 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). The full list is in Figure 7.7.

Figure 7.7: Top skills requested for core cyber job roles



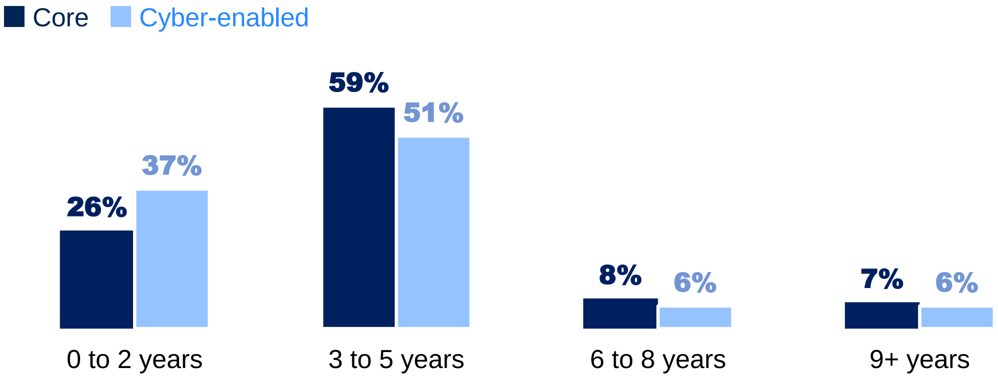
Source: Burning Glass Technologies
Base: 35,103 core cyber job postings from January to December 2021 that request at least one specific skill
*TCP or IP stands for Transmission Control Protocol (TCP) or Internet Protocol (IP).

Experience requirements

Figure 7.8 demonstrates that, over the last year, the most common request from employers looking to fill core cyber security roles has been for applicants with 3 to 5 years of experience (59%), followed by entry-level applicants (26%). This preference for the 3 to 5-year group is in line with the previous study. It remains higher than in 2019 (reported in the 2020 publication), when 52 per cent of job postings were asking for this many years of experience.

Compared to core cyber roles, there is a greater demand for those in entry level positions when it comes to cyber-enabled job roles (37%, vs. 26% per cent of core cyber job postings). This pattern is also similar to previous years. In other words, there is a continued preference among cyber security employers to take on dedicated (i.e. core) cyber staff at a more experienced level, whereas there is more flexibility for new entrants to pursue cyber-enabled job roles.

Figure 7.8: Percentage of core and cyber-enabled job postings asking for the following levels of minimum experience (where any minimum requirement is identified)



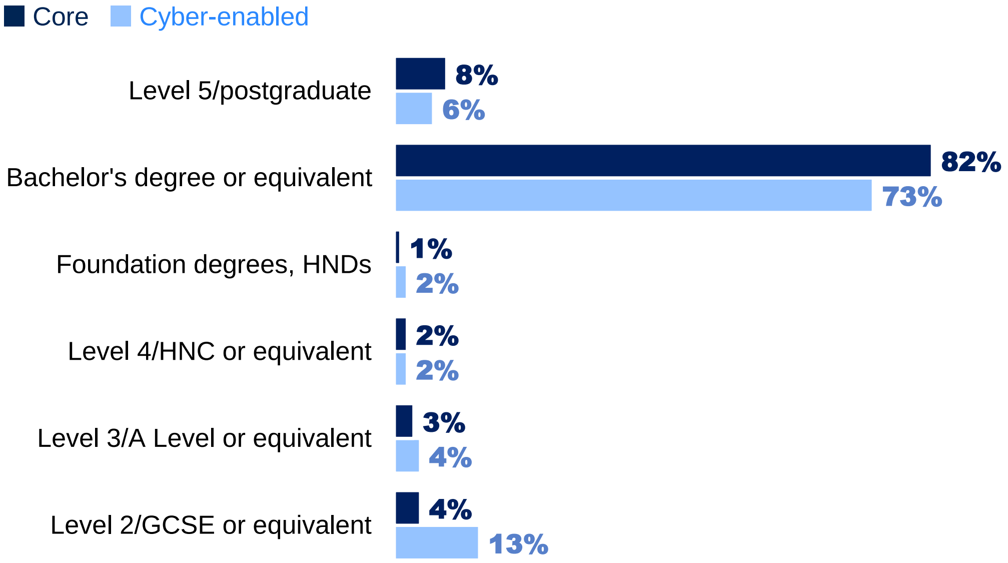
Source: Burning Glass Technologies
Bases (job postings that request specific experience from January to December 2021): 8,678 core cyber job postings; 22,629 cyber-enabled

Education requirements

As Figure 7.9 shows, employers continue to place a strong emphasis on applicants having bachelor's degrees or higher qualifications. In line with the previous studies, 90 per cent of employers expect a minimum of a bachelor's level degree (in a related subject) for core cyber security roles.

Employers seeking to fill cyber-enabled roles are more likely to accept A Levels or GCSEs (or their equivalents) as a minimum than core cyber roles (17% vs. 7%). Coupled with the fact that employers appear more willing to take on entry-level staff in cyber-enabled roles, these findings suggest that developing pathways for cyber-enabled IT and network roles could be a plausible, long-term way to increase the talent pool of more experienced individuals able to work in core cyber roles.

Figure 7.9: Percentage of core and cyber-enabled job postings asking for the following minimum levels of education (where any minimum requirement is identified)



Source: Burning Glass Technologies
Bases (job postings that have minimum education requirements from January to December 2021):
8,815 core cyber job postings; 21,657 cyber-enabled from January to December 2021

Demand for certifications

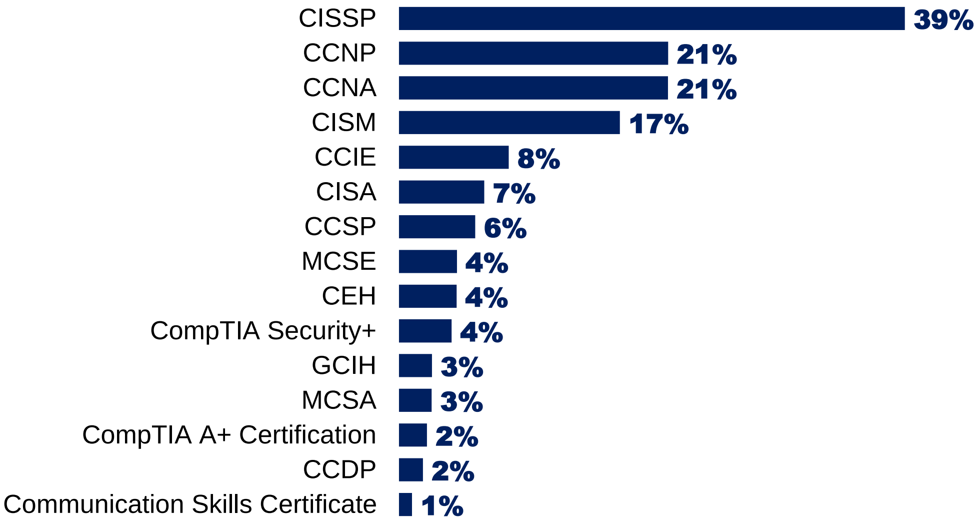
In previous waves of this research, the most commonly requested certification in job adverts has been the Certified Information Systems Security Professional (CISSP). This was included within 36 per cent of the job postings that ask for a specific certification last year. This year, the figure has increased further to 39 per cent of postings (Figure 7.10).

This year's qualitative research continues, in line with previous years, to suggest that:

- CISSP is a cyber security accreditation of which there is relatively wide awareness, making it more likely that employers will add this to job adverts
- It is viewed as one of the broader accreditations in cyber security, covering both the technical and governance aspects, making it popular for those looking to fill generalist roles

Figure 7.10 shows that Cisco Certified Network certifications also continue to be in high demand, with 21 per cent of job adverts requesting Cisco Certified Network Professionals (CCNP), 21 per cent requesting Cisco Certified Network Associates (CCNA), and 8 per cent requesting Cisco Certified Internetwork Experts (CCIE).

Figure 7.10: Percentage of core cyber job postings asking for the following certifications (where any certification is identified)



Source: Burning Glass Technologies
Base: 11,086 UK core cyber job postings from January to December 2021 that request specific certifications

7.7 Salaries

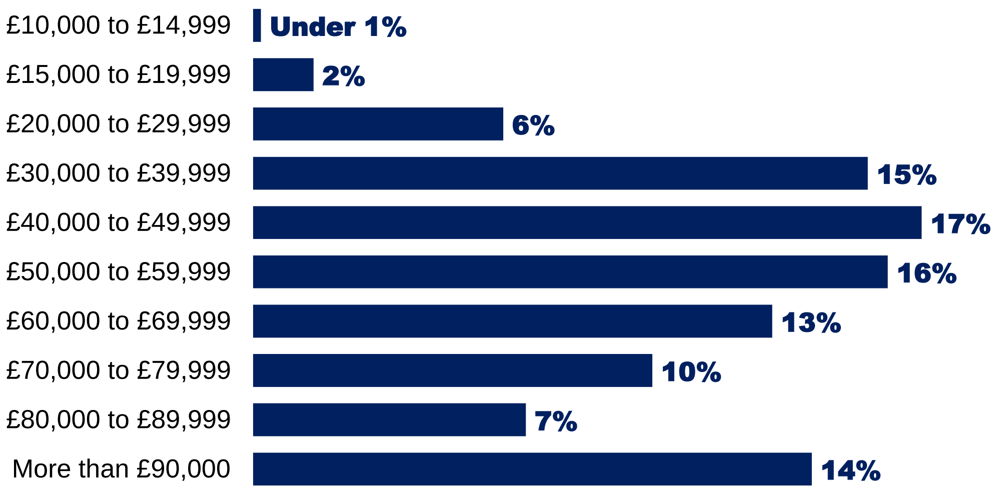
Across the 12 months of 2021, the average (mean) advertised salary was £60,100 for a core cyber job posting (with a median value of £55,000). This reflects a nominal mean increase of £900 (+1.5%) and nominal median increase of £2,000 (+3.7%) from 2020 levels.[18]

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 in 2021 was £48,369 (with a median of £40,000).[19] Using this value as a proxy for IT jobs in the UK suggests there is a wage premium of approximately 34 per cent for core cyber security jobs compared to IT jobs as a whole (when comparing median salaries).[20]

The mean advertised salary was £48,100 for all cyber job postings (i.e. including cyber-enabled job roles as well as core cyber roles), with a median of £40,500. This reflects no substantial change from last year (when we recorded a mean of £47,900 and a median of £40,700).

Figure 7.11 sets out the percentage of core cyber roles offering salaries within the following ranges, where the salary is advertised. The distribution is very similar to previous years. It is worth noting that around 55 per cent of online core cyber job postings do not contain any salary information.

Figure 7.11: Percentage of core cyber job postings offering the following salaries (where salary or salary range is advertised)



Source: Burning Glass Technologies
Base: 23,981 UK core cyber job postings from January to December 2021 that contain salaries or salary bands

[18] Our salary growth calculations do not account for inflation. The inflation data for 2021 has been skewed upwards due to various external factors, such as supply chain issues and physical access to stores, and wage growth across all sectors has not kept up. In future years, if inflation and wage growth continue to deviate, it may be important to reflect this in subsequent cyber security labour market reports.

[19] This is sourced from the Office for National Statistics (ONS, 2021 provisional data) Annual Survey of Hours and Earnings.

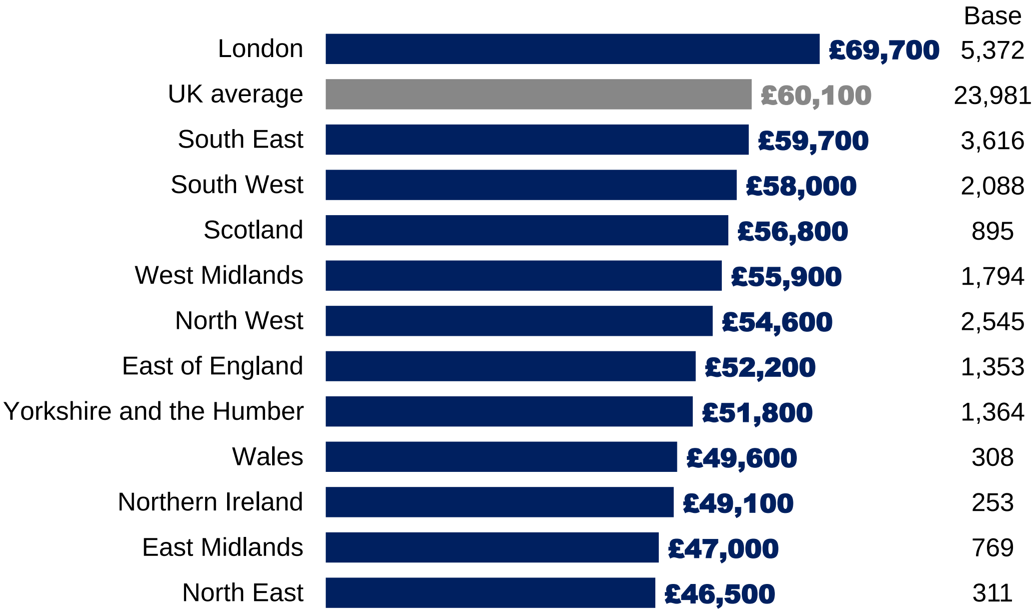
[20] This compared the median salary for core cyber job postings (£53,000) and all IT job postings (defined as SIC code 62, getting a median of approximately £41,000).

Geographical variation in salaries

London continues to have the highest mean advertised salary for core cyber roles, and is substantially ahead of all other regions, as Figure 7.12 shows. This is expected, given the prevalence of the professional services sector as well as higher typical costs of living in the capital.

There is a substantial variation in salaries across the regions. For instance, the difference between the mean salary in London and the North East for a core cyber job is £23,200. Even when taking the medians (not shown on the chart), there is a similar difference of £22,500 between London (£65,100) and the North East (£42,600).

Figure 7.12: Mean salary offers for core cyber job postings, by region (where the salary or salary range is advertised)



Source: Burning Glass Technologies
Bases as per chart (20,816 of the 23,981 job postings with salary data can be mapped to a specific UK region – the remainder are based in the UK but may include national or remote locations)

Changes over time

Table 7.1 provides an estimate of the change in advertised salaries at a regional level.

Any annual change in regional figures should be treated with caution and used in conjunction with other evidence. It may, for example, be especially skewed by any changes in advertised salary practices by larger employers.

Nevertheless, taken alongside the qualitative evidence from this study, the data in this table lends weight to the notion that employers across several regions have had to offer higher salaries in the wake of the pandemic, since it is now feasible for the local cyber security talent in their regions to apply to work remotely for employers in London and other higher paying regions.

The changes here could also more simply represent a return to the norms of 2019, before the pandemic. For example, in last year's report, we noted that the average (mean) salary in Wales had fallen by 13.1 per cent (from £51,000 in 2019, to £44,300 in 2020). This year, that drop has largely been reversed. This is also the case for the East of England and the North West, which saw average salaries drop last year but rise back this year. The West Midlands stands out in this regard – this region saw an increase of 4.5 per cent in average salaries this year (from £53,500 to £55,900), and saw a 4.9 per cent increase last year (from £51,000 in 2019, to £53,500 in 2020) as well.

Table 7.1: Change over time in mean salary offers for core cyber job postings by region (where salary is advertised)[21]

Region	2020	2021	Change since last year
Wales	£44,300	£49,600	£5,300 (+12.0%)
Scotland	£52,800	£56,800	£4,000 (+7.6%)
East of England	£49,800	£52,200	£2,400 (+4.8%)
West Midlands	£53,500	£55,900	£2,400 (+4.5%)
North West	£53,200	£54,600	£1,400 (+2.6%)
London	£68,000	£69,700	£1,700 (+2.5%)
Yorkshire and the Humber	£50,600	£51,800	£1,200 (+2.4%)
UK average	**£59,200**	**£60,100**	**£900 (+1.5%)**
Northern Ireland	£48,400	£49,100	£700 (+1.4%)
South East	£59,400	£59,700	£300 (+0.5%)
North East	£47,000	£46,500	-£500 (-1.1%)
South West	£59,900	£58,000	-£1,900 (-3.2%)
East Midlands	£48,600	£47,000	-£1,600 (-3.3%)

Qualitative findings on salary setting

The qualitative research suggests that employers aim to understand the market rate for salaries through a mix of conversations with their networks and recruitment agents, and by looking at other job postings online. When using the latter approach, it was evident in some cases that employers were looking at salaries in the wider IT labour market, rather than cyber security roles specifically. This was linked to the

[21] The salary figures in Table 7.1 are rounded to the nearest £100, while the per cent change amounts in the last column are based on the raw (non-rounded) data.

fact that these employers were recruiting for both cyber-specific roles and more general IT roles across their organisation or team.

Some public sector organisations highlighted that they could not afford to pay the market rate, which meant that they often could not attract the highest-quality candidates for cyber roles. This mirrors a concern about public sector pay caps raised in previous years.

A couple of key trends that were seen to have raised the market rates across the board were the high level of freelance work and a shift away from regional salary bands post-pandemic:

- Recruitment agents noted that freelancers in cyber security could typically demand high day rates, meaning this was often a more lucrative option for cyber professionals. This reduced the pool of labour vying for permanent contracts. One recruiter suggested that the diversified, large cyber consultancies had contributed strongly to this freelancer model, and thereby driven up market rates. Another said that the number of freelancers in the market had initially contracted after the changes to IR35 tax rules in April 2021, but had since returned to an equilibrium, with more people returning to the market as freelancers – and this had again led to market rates increasing
- As a result of the COVID-19 pandemic and the move to hybrid working, it was now much more common for people to apply for cyber roles across the UK and work remotely. Interviewees pointed out that this had led to market rate salaries being equalised across regions – this complements the findings around regional salary rises from the secondary data analysis. This was viewed as a considerable challenge for regional employers outside London, who would now have to pay higher salaries when recruiting or would need to attract candidates in other ways

> ***"I've just worked for a client based in Wales who had to compete with London salaries because their candidates were working remotely."***
> *Recruitment agent*

8 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 last year's report. In keeping with last year, the timeframe captured in these statistics is the last 18 months before the survey, which this time roughly equates to the start of January 2020.

Key findings

- A total of 11 per cent of the cyber workforce (within the cyber sector) are estimated to have left their posts since the start of 2020, with 9 per cent leaving of their own volition. These results suggest a higher staff turnover rate than in the previous year, when the estimate was 6 per cent
- The most common reason employers give for staff leaving of their own volition is due to uncompetitive pay or benefits (45% of the employers who have had staff leave)

8.1 An estimate of cyber workforce staff turnover

We estimate that 11 per cent of the cyber workforce (within the cyber sector) left their posts in the 18 months prior to the survey (i.e. since around January 2020). 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 is a higher staff turnover rate than the previous year's estimate (when it was 6%). In the qualitative strand, recruitment agents and some cyber employers suggested people were reluctant to change jobs during the pandemic, which would have dampened last year's staff turnover figure. This has now, perhaps, reverted to normal. At the same time, our job vacancies analysis highlights that demand for cyber security professionals has substantially shot up in the past year. The interaction of these two trends has led to a candidate-driven market, according to the recruiters we interviewed.

"People hunkered down during the pandemic while there was a lot of uncertainty. A lot of people who would have moved in that period are now on the market. There is a lot of movement, a lot of volatility."
Recruitment agent

"Those with the right amount of experience have realised that they are very much the commodity in the market. And they can be selective, which is why we have lots of passive candidates. They're happy to wait a long time and keep an eye on their emails, as they know they're in demand."
Recruitment agent

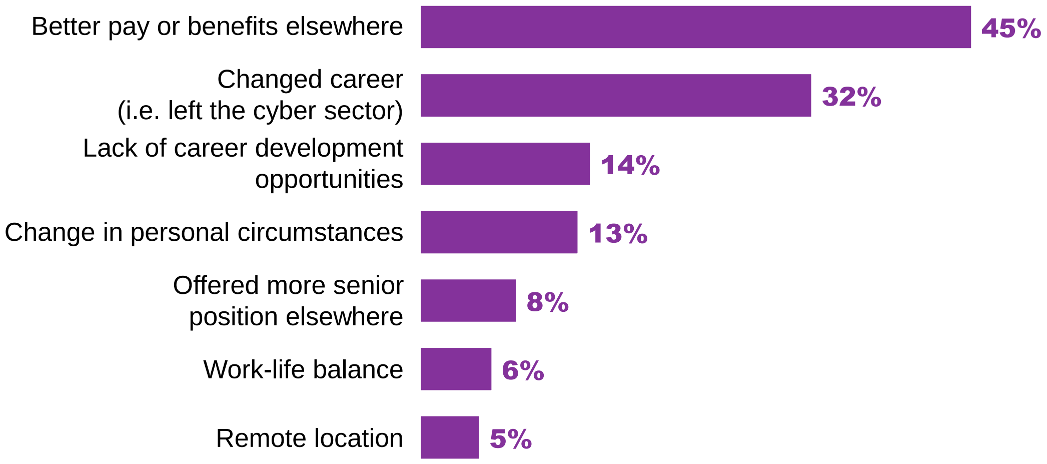
8.2 Why employees leave their roles

A total of 9 per cent left of their own volition, with the remaining 2 per cent being relatively equally distributed between retirement, redundancy as a result of COVID-19 and dismissal. This compares to 4 per cent leaving of their own volition in the previous study.

In the 9 per cent 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 8.1, 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 to get better pay or benefits elsewhere. This was also the biggest factor last year.

Figure 8.1: Reasons employers give for staff leaving cyber job roles, among those where any employees left of their own volition (unprompted – multiple answers allowed)



Base: 78 cyber sector businesses that have had employees leave since the start of 2020
Only specific categories mentioned by 5% or more shown.

There are changes from last year:

- The proportion saying their leavers exited the cyber sector entirely has risen (from 12% to 32%)
- Work-life balance was not one of the spontaneous response areas mentioned last year, whereas 6 per cent mention it this year
- Last year, 18 per cent said staff had relocated to another geographic area, whereas this year this response (which is distinct from the "remote location" response) does not factor. This reflects both the qualitative evidence and findings from the job vacancies analysis, suggesting that where staff are based is much less of an issue than before in an age of remote and flexible working. For example, one cyber firm based in South Wales talked about having people working for them from Bristol and Cheltenham

Lack of career development opportunities remains one of the mix of factors appearing unprompted. This complements the qualitative findings, which suggest that training and development opportunities are undervalued by some hiring managers in cyber security as a way of improving staff retention.

9 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.

Key findings

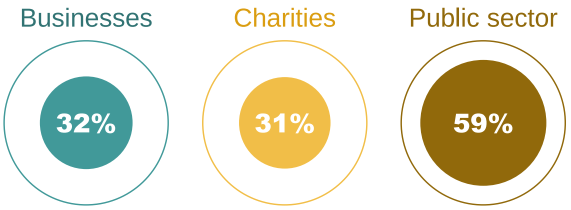
- Around 1 in 3 businesses (32%) outsource any aspects of cyber security, which is down from the previous year (when it was 38%). Outsourcing cyber security remains much more common in the public sector (at 59%)
- Setting up firewalls, detecting and removing malware, and incident response or recovery are the 3 most commonly outsourced cyber security functions. Among the 32 per cent of firms that outsource cyber security, 54 per cent 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 (15%). They are more common among large businesses (30%) and public sector organisations (33%)

9.1 The prevalence of outsourcing

Around a third of businesses outsource any aspects of cyber security (Figure 9.1). This proportion is similar among charities and higher among public sector organisations.

The business figure (32%) is down from 2021 (when it was 38%). This drop is driven by micro and small businesses specifically – the estimates for larger businesses are unchanged (58% of medium businesses and 57% of large businesses outsource).

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



Bases: 947 businesses; 211 charities; 123 public sector organisations

Outsourcing of cyber security functions remains more prevalent in the finance and insurance sector (59%, vs. 32% overall), which has been a consistent trend for the previous 2 years. Food or hospitality businesses are among the least likely to outsource cyber security (13%). Businesses in the South West are also less likely than average to outsource (20%), although this regional difference is not consistent with previous years.

9.2 What aspects of cyber security do organisations outsource?

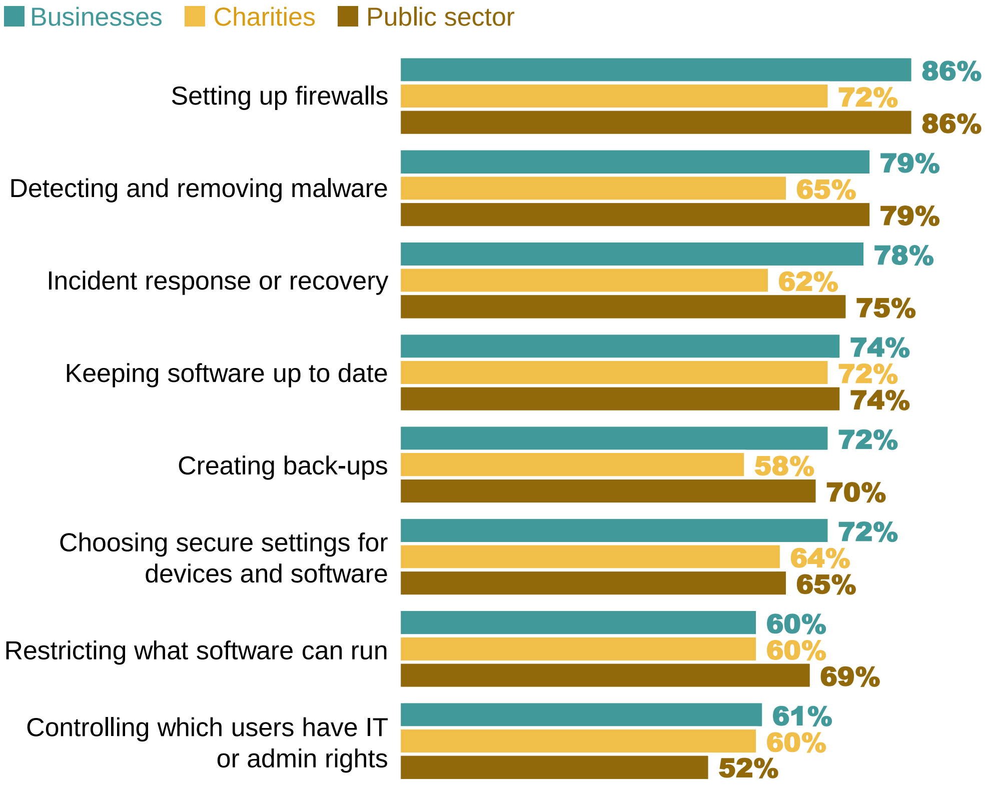
Outsourcing of basic functions (including incident response)

Figure 9.2 shows the kinds of basic functions (as opposed to the more advanced functions covered in the next sections) that get outsourced, among the organisations that outsource any aspects. The filtered charities and public sector samples are relatively small at 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 both previous years.

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 31 per cent of businesses, 33 per cent of charities and 38 per cent 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): 398 businesses; 90 charities; 70 public sector organisations

Use of Security Operations Centres (SOCs)

The use of Security Operations Centres (SOCs) remains consistent with previous years. A total of 16 per cent of businesses and 14 per cent of charities use one. This is higher among large businesses specifically (30%) and public sector organisations (33%). These results are consistent with last year, when this question was first asked (when 15% of businesses said they used SOCs).

Outsourcing of other more advanced functions

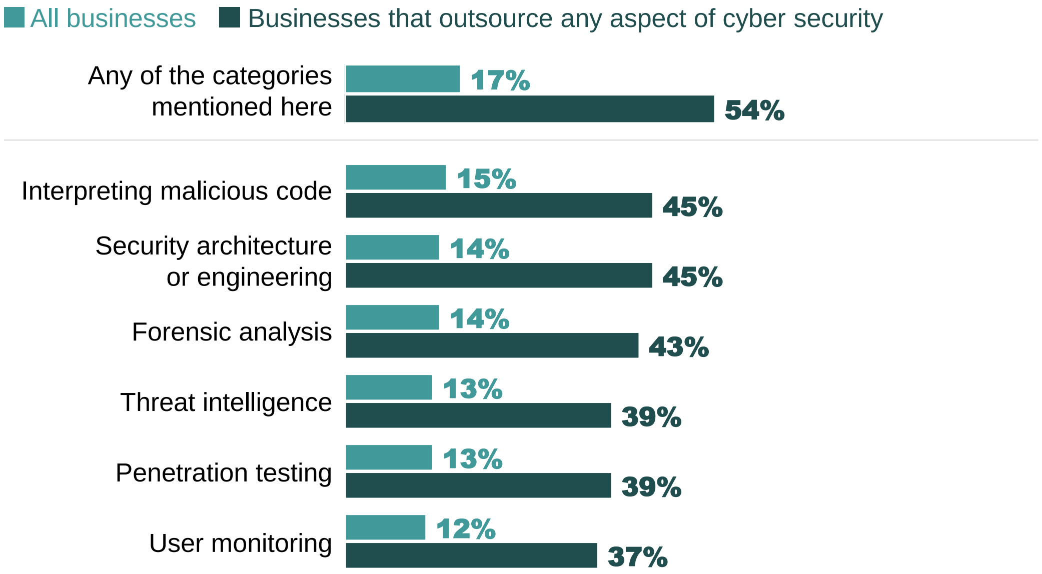
Figure 9.3 shows the other kinds of advanced functions that get outsourced. We show these results as a proportion of the 32 per cent of businesses that outsource any aspects of cyber security, as well as percentage of all businesses (i.e. including those who do and do not outsource).

In total, just under 1 in 5 businesses (17%) outsource any of these advanced cyber security functions. This proportion is considerably higher among large businesses (41%). There are too few public sector organisations and charities in our sample to analyse for this question.

The 6 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 these 6 categories – no single area is especially more likely to be outsourced than others. Interpreting malicious code was the top category by a small margin in the 2 previous studies as well.

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



Bases: 947 businesses; 265 businesses that outsource cyber security

10 The supply of cyber security skills

Previously, DCMS published research that explored the UK cyber security recruitment pool. This 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 covering 2020. This section provides a minor update to these estimates using the latest (i.e. 2021) data, wherever possible.[22] In addition, this strand produces further statistics on the characteristics of the recruitment pool, in terms of:

- Demographic diversity
- The geographic location of graduates
- Their educational and occupational backgrounds (e.g. based on course titles)
- Their salary bands
- An estimation of inflows into and outflows from the recruitment pool, informing a calculation of the overall cyber workforce gap (the annual shortfall of people working in cyber roles)

There is limited change in some of the headline figures when compared to the previous year's analysis – these figures are expected to remain relatively consistent over 1 to 2 years. However, even incremental changes can result in significant labour market changes in the long run.

As with the job vacancies analysis (Chapter 7), there are often very subtle differences in the data taken from big datasets. For this reason, we report some of the findings in this chapter to 1 decimal place, to show these subtle variations more accurately.

Key findings

- For 2021, we estimate the UK cyber security workforce to be in the region of c.110,000 to c.152,000, with a midpoint estimate of c.131,000. The 2020 estimate was c.134,500. This suggests there has been no substantial change in the total size of the workforce since last year
- A total of c.7,500 individuals entered the cyber security workforce in 2021, which is similar to the 2020 inflow. In subsequent years, this inflow may increase, subject to a growth in participation in retraining initiatives
- Around 3.5 per cent of the cyber security workforce left the profession entirely in 2021. This suggests an estimated outflow of c.4,600 leavers per year
- Employment in the cyber security sector has increased by 13 per cent within the last year. This suggests a need for c.17,000 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.21,600 per year
- Taken together, these findings suggest a net annual shortfall of c.14,100 people in 2021. This is an increase of c.4,100 from the 2020 estimate

10.1 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. We made a bespoke data request for cyber security and computer

[22] We do not provide an update to the further education or apprenticeships data covered in the previous recruitment pool research, as the latest annual data for these will not be published in time for this report. The role of certification and private training providers outside the state education sector is also not updated in this report, having been comprehensively covered in the previous work (see Section 3.5 of the recruitment pool report).

science enrolments and outcomes covering 3 academic years (2017/18, 2018/19 and 2019/20). This expands on the analysis in the previous recruitment pool report to add the most recent published data, which in some instances covers the 2018/19 academic year or the 2019/20 academic year.

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)

In recent years, 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).

Courses

Table 10.1 shows the number of courses offered by UK Higher Education institutions in cyber security and computer science[23] (based on unique course titles offered in 2018/19 and 2019/20).

Table 10.1: Number of cyber security and computer science courses and providers (2018/19 and 2019/20 academic years)

Qualification level	Cyber security	Computer science
Undergraduate (First Degree)	262 (from 66 universities)	2,020 (from 124 universities)
Other undergraduate (e.g. Foundation)	7 (from 7 universities)	150 (from 52 universities)
Postgraduate	213 (from 76 universities)	1,648 (from 124 universities)
Total	**482**	**3,818**

Overall, we identified 66 universities offering undergraduate courses and 76 universities offering postgraduate courses in cyber security. In recent years, dedicated cyber security courses within UK universities have often been offered at Master’s level, following completion of a relevant Bachelor’s degree in a related subject such as computer science. However, there has been a notable increase in the number of universities offering dedicated cyber security courses at Bachelor’s level in the latest 12 months of data (up from 239 in the 2018/19 academic year to 262 in 2019/20).

Tables 10.2 and 10.3 provide an update (from the previous cyber recruitment pool report) for 2019/20, in terms of student enrolment and qualifiers for cyber security and computer science courses.[24]

Table 10.2: Breakdown of student enrolment and qualifiers in cyber security courses in UK Higher Education institutions (HEIs, 2018/19 and 2019/20 academic years)

	Number of HEIs offering a relevant course		Number of students enrolled		Number graduating	
Academic Year	2018/19	2019/20	2018/19	2019/20	2018/19	2019/20
Undergraduate	64	66	8,670	10,070	2,060	2,140

[23] These two groups of courses are mutually exclusive, i.e. there is no overlap between the groups.

[24] The numbers in the tables are rounded to the nearest 10, so do not sum to the totals (due to rounding).

Postgraduate	73	76	3,020	3,620	1,310	1,460
Total	**83**	**87**	**11,690**	**13,680**	**3,360**	**3,600**

Table 10.3: Breakdown of student enrolment and qualifiers in computer science courses in UK Higher Education institutions (HEIs, 2018/19 and 2019/20 academic years)

	Number of HEIs offering a relevant course		**Number of students enrolled**		**Number graduating**	
Academic Year	2018/19	2019/20	2018/19	2019/20	2018/19	2019/20
Undergraduate	122	126	89,760	96,970	21,000	20,770
Postgraduate	121	124	21,050	29,730	9,890	11,560
Total	**128**	**131**	**110,820**	**126,690**	**30,890**	**32,330**

These tables show that, in the most recent available year (2019/20), the number of individuals enrolled in cyber security courses has increased by 17 per cent and the number of cyber security graduates has increased by 7 per cent. Furthermore, computer science enrolments have also increased by 14 per cent, and the number of computer science graduates has increased by 5 per cent.

This increase is likely to support the narrowing of the cyber workforce gap in the long run. However, it is still a small increase within the context of known skills gaps across the UK economy.

Student profiles

This section updates the breakdown of graduates in cyber security and computer science courses from the cyber recruitment pool report for the latest year of available data (2019/20), in terms of gender identity, ethnicity, domicile, age and entry from state schools.

- The cyber sector workforce is estimated to have a disproportionately low number of female staff, as Chapter 3 shows. This gender gap persists in the Higher Education recruitment pool. The 2019/20 data suggests that only 12 per cent of undergraduate and 17 per cent of postgraduate students studying cyber security courses are female, reflecting no change from the previous year

- An estimated 24 per cent of students enrolled in a cyber security course, and 19 per cent of computer science students were from an ethnic minority background. These are likely to be bare minimum estimates – 20 per cent of cyber security students and 30 per cent of computer science students have their ethnicity listed as unknown, and a high proportion of these are likely to be ethnic minority international students. This outlook is also unchanged from the previous year

- In 2018/19, an estimated 63 per cent of students were from the UK, 7 per cent were from EU countries, and 29 per cent from outside of the EU, demonstrating the significance of international students in the UK. The prevalence of international students is highest among the postgraduate population. And in 2019/20, the importance of international postgraduate students has increased further, with non-EU students now accounting for 38 per cent of cyber security postgraduates

- In 2019/20, there continued to be significant demand for cyber-related courses from mature students (aged 25 and over). A total of 11 per cent of cyber security undergraduate students and 42 per cent of cyber security postgraduate students are aged 30 and over. For computer science courses, this is 11 per cent and 25 per cent respectively (for undergraduates and postgraduates)

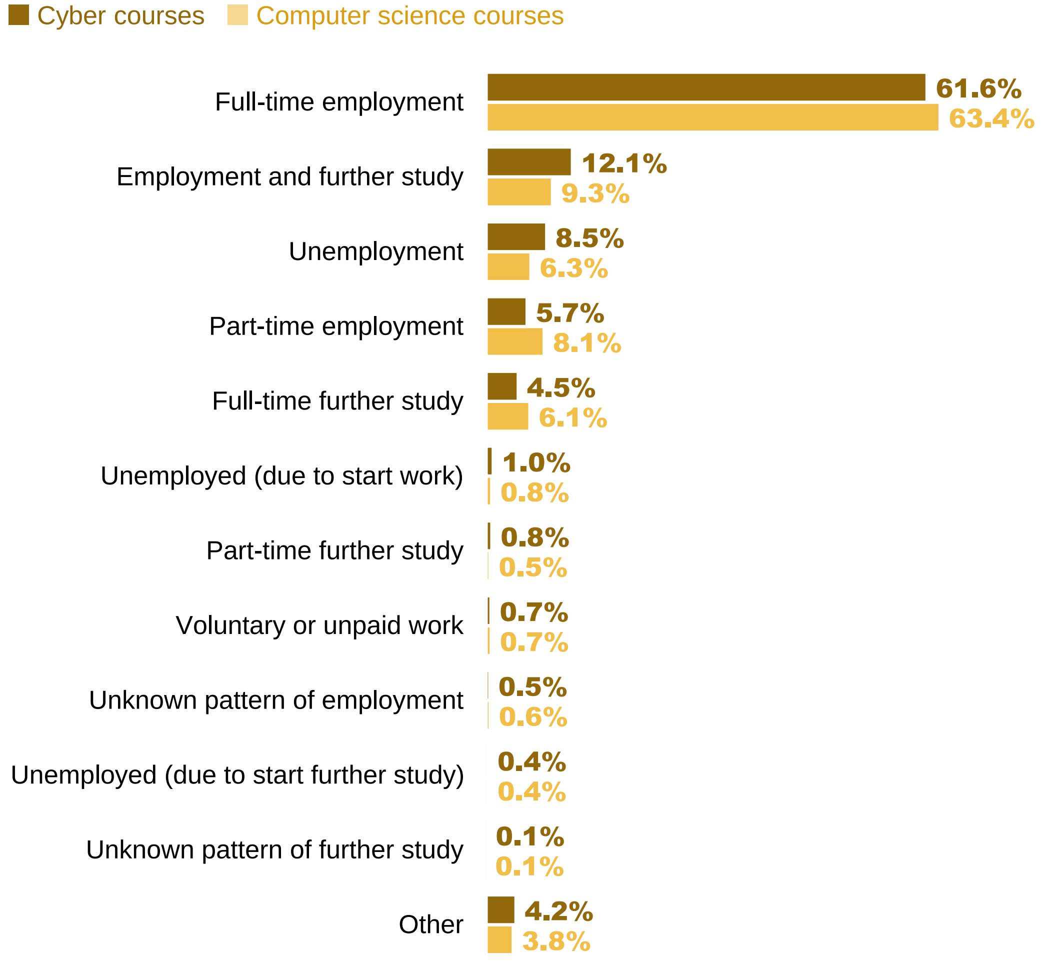
- The 2019/20 data for students coming from state-funded schools is less reliable, given a high proportion where the school type is unknown (around 3 to 4 in 10). However, there is no evidence to suggest a significant change from the 2018/19 results, which showed 85 per cent of cyber security students and 69 per cent of computer science students coming from UK state schools

Graduate outcomes

The latest available HESA data on graduate outcomes covers the 2018/19 academic year (providing an update to the 2017/18 data covered in the previous cyber recruitment pool report). The data is based on responses to HESA's Graduate Outcomes survey, which may not fully cover certain groups of the graduate population (e.g. those returning to another country following completion of studies in the UK).

Figure 10.1 shows the overall graduate outcomes for those that graduated in the academic year 2018/19. Graduates are asked information about their activities approximately 15 months after they complete their studies, so the responses received can show activity taking place between December 2019 and September 2020 (i.e. before and after the COVID-19 pandemic restrictions in the UK).

Figure 10.1: Overall graduate outcomes (2018/19 academic year)



Source: Jisc and HESA Graduate Outcomes (2018/19 cohort)
Bases: 1,610 cyber graduates; 15,560 computer science graduates

This indicates that approximately 62 per cent of cyber security graduates enter full-time employment, with a further 12 per cent blending employment and further study. A further 6 per cent entered part-time employment. This means that, of the 3,600 students that graduated within a cyber security course in 2018/19, we expect that approximately 80 per cent should enter or stay within employment within 15 months of graduation since their most recent degree award.

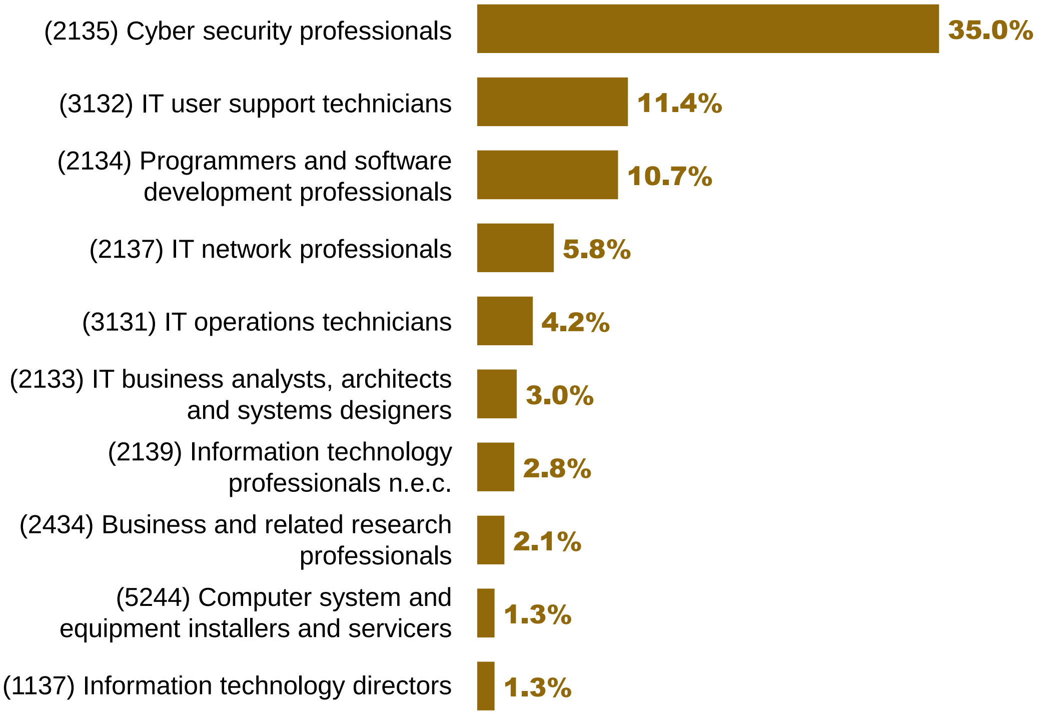
The cyber security course figures are comparable for other computer science courses. In both cases, overall employment rates are also similar to the previous year. This suggests that cyber security and computer science graduate employment has remained, broadly, consistent despite the COVID-19 pandemic.

Nevertheless, there is evidence that the pandemic has made it harder for some graduates to find work. A total of 8.5 per cent of cyber security graduates in this cohort reported being unemployed (with no expectation of a new job or further study). This is higher than the previous year (6.5%).

Employment outcomes

The Graduate Outcomes survey now uses Standard Occupational Classification (SOC) 2020, which for the first time includes a distinct identifier for cyber security professionals. As shown in Figure 10.2, around a third (35%) of cyber security graduates with full-time employment status have moved into a cyber security professional role within 15 months of graduating. Most of the remaining graduates that move into full-time employment tend to go into an IT-related role (accounting for 43% of the remaining SOC codes), which could include the need for technical and non-technical cyber security skills.

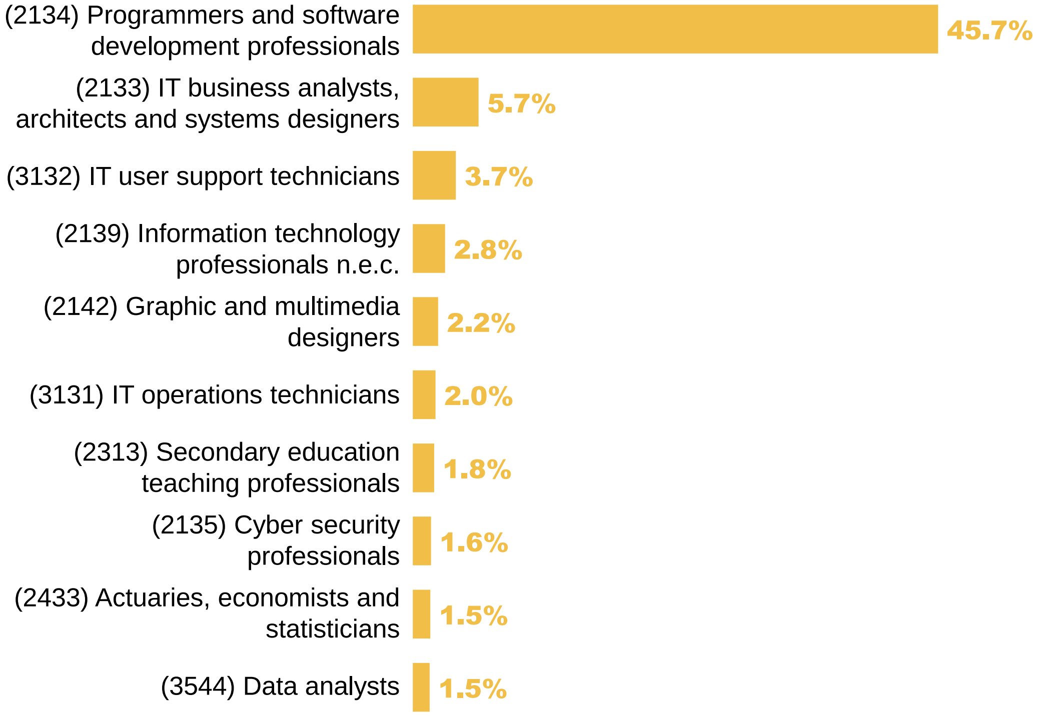
Figure 10.2: Top job roles based on Standard Occupational Classification (SOC) 2020 for cyber security graduates (2018/19 academic year)



Source: Jisc and HESA Graduate Outcomes (2018/19 cohort)
Base: 1,610 cyber graduates in full-time employment
Standard Occupational Classification (SOC) 2020 code listed in brackets

For those graduating in computer science that have entered a full-time role (Figure 10.3), just under half (46%) report that they are currently involved in a programming and software development role. Only 2 per cent report being within a cyber security professional role. However, it worth noting that there are approximately 10 times the volume of computer science graduates as cyber security graduates in the UK, so this 2 per cent still reflects an important driver for cyber security graduate employment.

Figure 10.3: Top job roles based on Standard Occupational Classification (SOC) 2020 for computer science graduates (2018/19 academic year)



Source: Jisc and HESA Graduate Outcomes (2018/19 cohort)
Base: 15,560 computer science graduates in full-time employment
Standard Occupational Classification (SOC) 2020 code listed in brackets

With respect to the cyber recruitment pool, we assume that the following number of Higher Education graduates may be likely to enter IT and cyber security roles each year (Tables 10.4 and 10.5):

Table 10.4: Estimated number of graduates moving into IT-related roles

Course type	Number of graduates	Proportion in full-time employment	Proportion of those in IT roles	Implied population
Cyber security	3,600	62%	90%	2,000 (rounded)
Other computer science	32,330	63%	80%	16,500 (rounded)
Total				**18,500**

Table 10.5: Estimated number of graduates moving into cyber security professional roles

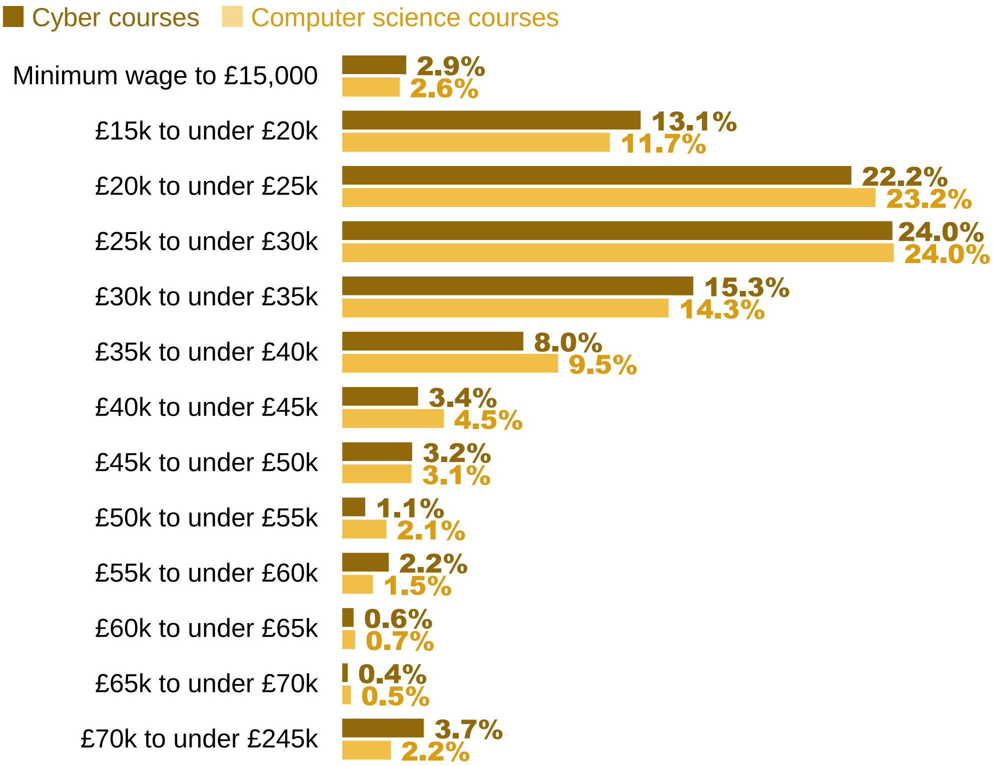
Course type	Number of graduates	Proportion in full-time employment	Proportion of those in SOC 2135 (cyber)	Implied population
Cyber security	3,600	62%	35%	800 (rounded)
Other computer science	32,330	63%	2%	400 (rounded)
Total				**1,200**

The previous cyber recruitment pool research estimated that c.2,000 cyber security graduates, and a further c.2,000 computer science graduates may be likely each year to enter a cyber security role. The introduction of the SOC 2020 code for cyber security professionals suggests a lower figure of c.1,200. However, this does not include where respondents may be involved in programming or networking roles aligned to cyber security. Therefore, rather than using the revised estimate of 1,200, we have kept the previous estimate of 4,000 as our estimated inflow from the Higher Education sector into the broader cyber security labour market each year.

Salaries

Analysis of Graduate Outcomes data also indicates salary bands for those in full-time employment. Figure 10.4 shows that the earnings of graduates from cyber degree courses broadly matched the earnings of graduates from computer science courses (see figure below). Around two-thirds of graduates from both courses were earning less than £30,000 within 15 months of graduating.

Figure 10.4: Reported salaries by those in full-time equivalent employment (2018/19 academic year)



Source: HESA Graduate Outcomes (2018/19 cohort)
Bases: 790 cyber graduates; 7,390 computer science graduates

10.2 Estimating the size of the cyber security recruitment pool

The previous cyber recruitment pool research drew an estimate of c.134,500 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.

A note on the ISC2 Cybersecurity Workforce Study estimate

The 2021 ISC2 Cybersecurity Workforce Study suggests there are c.301,000 individuals in the UK cyber security workforce, with a shortage of c.33,000. It is not possible for us to validate their estimate with our data, given the vast differences in methodologies between our two studies (outlined later in this section) and a lack of published technical information on the UK sample size and representativeness of the ISC2 data. The estimate is also likely to have a substantive margin of error around it.

The ISC2 estimate has fluctuated considerably across years, from c.289,000 in 2019 and c.366,000 in 2020. In our opinion, it remains unrealistically high. It would mean that almost 1 in every 100 employees in the UK are working in a cyber role. Furthermore, the DCMS Sectors Economic Estimates indicate that there were c.1.8 million jobs across all UK digital sectors from July 2020 to June 2021. If the ISC2 estimate was correct, this would mean that around 1 in 6 digital sector jobs are in cyber security.

DCMS Cyber Security Sectoral Analysis workforce growth estimate

Since 2017, DCMS 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 10.6.

In the most recent year, employment in the cyber security sector has grown by 13 per cent, and the sector has experienced double-digit growth in previous years (outside 2020).

Table 10.6: Number of full-time equivalent employees within the UK cyber sector

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

Tech Partnership workforce baseline estimate

In 2017, the Tech Partnership published that the UK cyber security workforce had reached 58,000 professionals by the end of 2016, which was a significant increase from 22,000 in 2011 (160% growth over the 5-year period, or 14% per year).

This research reflected those in salaried employment across the public and private sectors, and Tech Partnership estimated that approximately 12 per cent of cyber security roles were within the UK public sector. This compares to 16 per cent of all people in paid work being in the public sector, suggesting that cyber security roles in the UK may skew slightly more to the private sector.

The previous cyber recruitment pool exercise estimated that the cyber security workforce may have reached 98,000 people by the end of 2020 using the Tech Partnership baseline and assuming average annual growth of 14 per cent per year from 2016 to 2020. Extending this to the end of 2021, and applying the DCMS sectoral analysis growth figure of 13 per cent from 2020 to 2021 suggests a figure of c.110,000 individuals.

A maximum estimated cyber security workforce based on job vacancies

The previous cyber recruitment pool exercise attempted to estimate the maximum possible cyber security workforce by:

- Using job vacancies data (covered in Chapter 7) to calculate the ratio of cyber security employees within the cyber sector to those outside the cyber sector
- Applying this ratio to the number of FTEs working within the cyber sector, to estimate the number of FTEs in cyber-enabled roles outside the cyber sector

To calculate the ratio, we have assumed that:

- The core cyber security job vacancies (from Chapter 7) are predominantly to fill roles within the cyber sector, which has the greatest demand for people with these high-level technical cyber skills
- The cyber-enabled job vacancies (also from Chapter 7) are predominantly representing the people employed in cyber roles outside the cyber sector

For 2020 job vacancies, this ratio was 2.67. In other words, we estimated that for every cyber security job vacancy within the cyber sector, there were a further 2.67 cyber security vacancies in the wider economy. The 2021 job vacancies data suggests this ratio has fallen, due to increased demand for core cyber security roles, which we assume are more likely to be placed within the cyber sector. In chapter 7, we identified that there were, on average, c.4,400 core cyber security roles posted each month in 2021, compared to c.8,300 cyber-enabled job roles per month. This yields a ratio of 1.9.

Multiplying this ratio by the most recent estimate of FTEs within the cyber sector (52,727) provides an overall maximum estimated size for the cyber security workforce outside the cyber sector, of c.99,000.[25] This means the total maximum estimated size of the cyber security workforce within the cyber sector (c.53,000) and outside the cyber sector (c.99,000) is c.152,000.[26]

This is around 10 per cent lower than the previous year's estimate (of c.171,000).

Overall workforce estimation scenarios

In absence of SOC data at the population level, it is challenging to identify the number of people working within a cyber security role within the UK. However, our estimates suggest:

- There are at least 110,000 individuals in these roles based on industry growth (measured in the annual DCMS Cyber Sectoral Analysis) and the Tech Partnership baseline
- There are at most 152,000 individuals in these roles based on the ratio of cyber roles within the cyber sector to those outside the cyber sector

Therefore, for 2021, we estimate the size of the UK cyber security workforce to be in region of c.110,000 to c,152,000, with a midpoint estimate of c.131,000. This suggests no substantial change in the total size of the workforce over the last 12 months, given that our previous midpoint estimate (from the cyber recruitment pool report) was 134,500.

[25] This is a high-end estimate, as we know that not all the 52,727 FTEs within the cyber sector are people working in cyber roles. They will also include a number of people in non-cyber roles (e.g. in diversified companies), as well as administrative staff.

[26] We have carried out these calculations using non-rounded ratios, then rounding the results to the nearest 1,000. The calculations are laid out in full in the separate technical report.

10.3 Estimating the cyber security workforce gap

The previous cyber recruitment pool research indicated a shortfall of c.10,000 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 13,700 individuals a year (an increase of 3,700). The constituent parts of this calculation are as follows, bringing together the estimates from the rest of this chapter:

- For 2021, we estimate the current workforce to be in the region of c.110,000 to c.152,000, with a midpoint estimate of c.131,000

- A total of c.7,500 individuals entered the cyber security workforce in 2021. 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 1,000 involved in apprenticeships in cyber security. The latter 2 figures (2,500 retraining and 1,000 apprentices) are taken directly from the cyber recruitment pool research and have not been updated, as they are still based on the latest published data

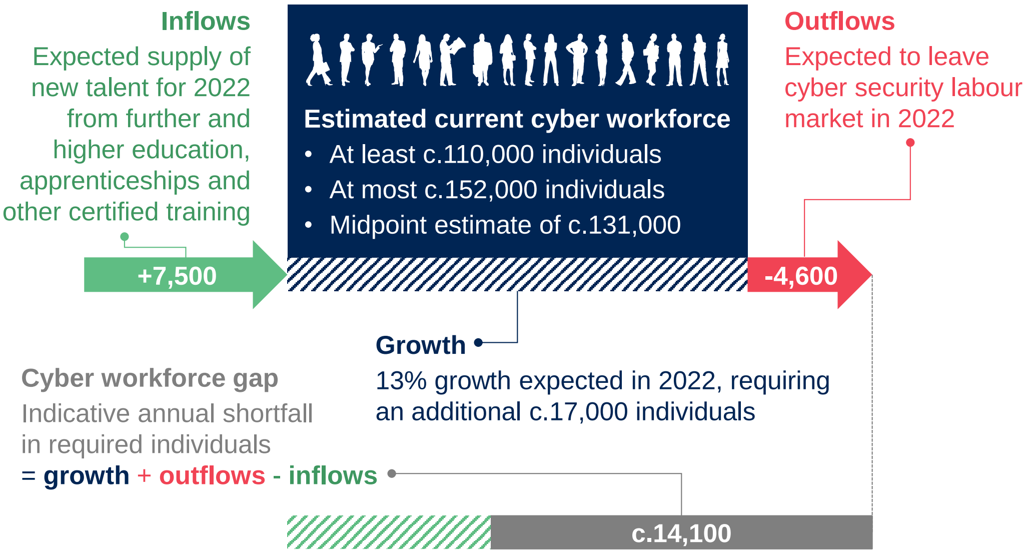
- As Chapter 8 shows, up to 11 per cent of the current cyber workforce (within the cyber sector) left their employer for any given reason in 2021. Of these, an estimated 32 per cent completely left the sector. Extrapolating from this to the entire cyber security workforce, we therefore estimate an outflow of 3.5 per cent (vs. 4% in 2020), giving a midpoint estimate of c.4,600 leavers each year

- Employment in the cyber security sector has increased by 13 per cent within the last year according to the DCMS Cyber Sectoral Analysis 2022. This suggests a need for c.17,000 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.21,600 per year

- Taken together, these findings suggest a net annual shortfall of c.14,100 people in 2021. This is an increase of c.4,100 from the 2020 estimate

Figure 10.5 concludes with a visual summary of this workforce gap, updating the one produced in the cyber recruitment pool research.

Figure 10.5: Visual summary of 2021 cyber workforce gap


Inflows
Expected supply of new talent for 2022 from further and higher education, apprenticeships and other certified training
+7,500
Estimated current cyber workforce
• At least c.110,000 individuals
• At most c.152,000 individuals
• Midpoint estimate of c.131,000
Outflows
Expected to leave cyber security labour market in 2022
-4,600
Growth
13% growth expected in 2022, requiring an additional c.17,000 individuals
Cyber workforce gap
Indicative annual shortfall in required individuals
= growth + outflows - inflows
c.14,100

11 Conclusions

For the first time, this report brings together the most comprehensive data on the supply side and the demand side of UK cyber skills gaps and shortages. It highlights the immense challenge in meeting employers' recruitment and training needs. And from the perspective of individuals entering or active in the cyber security labour market, it illustrates the difficulties they face finding the right career and training pathways, and the increasing need for a holistic skillset in various roles.

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 number of organisations providing cyber security training (for cyber teams and wider staff) – a minority outside the cyber sector
- The specific skills areas, roles and seniority levels seen as hardest to fill – although there are now higher reported skills gaps in the cyber sector, relative to 2021, in operational security management and implementing secure systems
- 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, touching on the following themes:

- The perceived shortcomings of available training and qualifications
- A lack of awareness and uniformity around professional development pathways, and a lack of time for people outside the cyber sector to dedicate to Continuing Professional Development (CPD)
- Poorly written job specifications, sometimes the result of poor communication between hiring managers, HR staff and recruitment agents

For this reason, the 9 recommendations laid out in last year's report still stand, and government and industry should continue their efforts in these areas. In addition, we acknowledge the helpfulness of new tools like the UK Cyber Security Council's Careers Route Map, which met with positive feedback in our interviews. It will play an important role in shaping employers' and individuals' understanding of possible career pathways into and within the cyber security labour market.

Nevertheless, this year's study also paints a detailed picture of an evolving cyber security labour market, with a rapid and substantial growth in demand for cyber skills, changes in the ways roles are advertised and recruited, an increasing interest in effective, holistic training approaches to build people's confidence and skills, and a potentially heightened awareness of workforce diversity issues. With this in mind, the newest insights from this 2022 report are as follows:

- **The demand for cyber security professionals has increased significantly in 2021.** This continues and surpasses the post-pandemic recovery in demand seen in autumn 2020. Employers and recruitment agents consider the cyber security labour market an increasingly candidate-driven market, with a greater average number of vacancies per firm this year, and a greater proportion of these vacancies being hard to fill. In this context, our estimate of the cyber workforce gap – the annual shortfall in cyber security personnel – has slightly increased (to 13,700) from the earlier estimate in DCMS's cyber recruitment pool research

- **The COVID-19 pandemic and resulting changes to working practices continue to bring opportunities and challenges to the cyber security labour market.** With the ability to work remotely in many cyber roles, employers are more agnostic about where their cyber employees are based. This is expected to have a positive impact on workforce diversity. On the other hand, the evidence suggests it has led to market rate salaries for cyber roles being equalised across regions, presenting challenges for smaller, regional employers. In addition, for some of those in IT roles covering cyber security functions, the pandemic has continued to add to workloads, meaning that training and development in the cyber security area has sometimes been put on hold

- **There are early-stage indications that the cyber sector is increasingly taking on entry-level staff.** A higher proportion of cyber sector firms are recruiting via graduate schemes. While this remains more prevalent in larger firms, the emerging pattern across 3 years of data suggests that a wider range of employers are taking on career starters than before and providing introductory training for new joiners. Further years of data will help to validate this indicative trend

- **Over the last 3 years, cyber sector firms have evolved their recruitment approaches.** These firms have reduced their use of recruitment agents and moved more towards recruiting via social networks (such as LinkedIn). In addition, there was less direct recruitment via online job adverts in the cyber sector in 2021. A greater share of these online job adverts was taken up by the broader IT sector (excluding firms offering cyber products or services), consultancies and the public sector

- **A lack of complementary skills among job applicants has become a bigger issue for cyber sector businesses this year.** A total of 4 in 10 now say that job applicants are deficient in their complementary skills. This includes communication, leadership, management, and sales and marketing skills, as well as the ability to write well. Outside the cyber sector, the ability to influence others' behaviour around cyber security remains an important skill, in line with last year

- **More businesses this year find themselves lacking incident management skills.** Outside the cyber sector, across the wider economy, technical cyber skills gaps have remained relatively constant – half of all firms lack basic skills and a third have more advanced skills gaps (in areas such as penetration testing, forensic analysis and security architecture). However, across the last 3 years of data, the proportion of businesses saying they are not confident dealing with a cyber security breach or attack has risen from around a quarter to closer to 4 in 10

- **The perceived effectiveness of cyber security training for those in cyber roles outside the cyber sector has fallen this year.** Among the non-cyber businesses providing training to this group, only around 1 in 10 say it completely met their needs. A strong theme in this year's research was the existence of low-quality cyber security training in the external training market, and the challenge of distinguishing good and bad training. Alongside this, we heard about the importance of ongoing training and mentoring, both as a way of attracting and retaining good cyber staff, and to build people's confidence to apply their technical skills effectively in the workplace

- **Among many businesses, workforce diversity is a higher profile issue in general than before, and there has been progress in diversifying the cyber workforce.** The proportions of the cyber sector workforce that are female and from ethnic minorities both appear to have increased across the past 3 years. In addition, there has been an increase in efforts to recruit people with neurodiverse conditions. These efforts are, however, a continual process. The existing pool of individuals that could potentially enter the cyber security labour market remains skewed towards men, highlighting a need for early intervention through initiatives like Cyber Explorers. And the lack of diversity in senior roles shows the ongoing importance of having advocates for diverse cyber recruitment, within organisations and across the industry. In this sense, the efforts of individuals, as well as industry-wide initiatives such as the Tech Talent Charter, both serve to engender a culture shift among employers and raise awareness of diverse candidates' needs

Appendix: regional findings summary

The UK government's National Cyber Strategy 2022 highlights the role that the cyber sector can play in levelling up each of the UK's 12 regions (including Northern Ireland, Scotland and Wales). To this end, it is important to understand the current state of the cyber security labour market within each region. This appendix brings together, in a single table, some of the regional findings from the job vacancies analysis (Figures 7.3 and 7.12 from Chapter 7) some of the regional findings from the DCMS Cyber Security Sectoral Analysis 2022. The sectoral analysis report contained 12 regional snapshots showing the geographic clustering of cyber security jobs within each region.

Summary of employment and job vacancies metrics by UK region, covering the previous calendar year (2021)

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)[27]	Percentage of all UK core cyber security job vacancies	Average (mean) advertised salaries in core cyber security roles
Greater London	1,095	29%	29%	12,647	30.3%	£69,700
South East	676	18%	16%	7,245	17.3%	£59,700
North West	339	9%	9%	4,446	10.6%	£54,600
South West	303	8%	8%	4,120	9.9%	£58,000
West Midlands	196	5%	7%	3,085	7.4%	£55,900
East of England	243	6%	6%	2,452	5.9%	£52,200
Yorkshire and the Humber	172	5%	5%	2,332	5.6%	£51,800
Scotland	323	8%	7%	2,231	5.3%	£56,800
East Midlands	149	4%	3%	1,232	2.9%	£47,000
North East	117	3%	2%	770	1.8%	£46,500
Northern Ireland	94	2%	4%	668	1.6%	£49,100
Wales	111	3%	4%	575	1.4%	£49,600
All UK						**£60,100**

[27] Based on 41,803 core cyber job postings on the Burning Glass labour market database from January to December 2021, where region was listed (out of the total 53,144 core cyber job postings in this period).

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.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos.com/en-uk
http://twitter.com/IpsosUK

About Ipsos Public Affairs

Ipsos Public Affairs works closely with national governments, local public services and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.