Cyber security skills in the UK labour market 2021

Findings report

Darragh McHenry, Tania Borges, Alex Bollen and Jayesh Navin Shah, Ipsos MORI
Sam Donaldson, Perspective Economics
David Crozier, Centre for Secure Information Technologies
Professor Steven Furnell, University of Nottingham

Department for
Digital, Culture
Media & Sport

Ipsos MORI

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

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 680,000 businesses (50%) have a basic skills gap. That is, the people in charge of cyber security in those businesses lack the confidence to carry out the kinds of basic tasks laid out in the government-endorsed Cyber Essentials scheme, and are not getting support from external cyber security providers. The most common of these skills gaps are in storing or transferring personal data, setting up configured firewalls, and detecting and removing malware
- Approximately 449,000 businesses (33%) have more advanced skills gaps, most commonly in areas such as penetration testing, forensic analysis and security architecture
- A third (32%) have a skills gap when it comes to incident response (and do not outsource this)

In qualitative interviews with these businesses, there was a sense that cyber security skills were poorly understood and undervalued, both among management boards and within IT teams. It was, therefore, very important for cyber leads to have the skills to be able to influence behaviour and culture within their organisations, and to discuss cyber security in terms of business risk with senior managers.

Outside the cyber sector, the more basic skills needs reflect the career pathways of those who end up working in cyber roles, with 86 per cent having transitioned from a previous non-cyber role. By contrast, in the cyber sector, half the workforce (49%) have previously worked in a cyber role elsewhere.

Nevertheless, skills gaps, both technical and non-technical, are also common in the cyber sector.

- Almost half (47%) of cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants. A total of 13 per cent say that job applicants having these skills gaps has prevented them from achieving business goals *to a great extent*
- Technical skills gaps were most commonly cited in the following 3 areas: incident management, investigation and digital forensics (41% of the firms identifying any technical skills gaps), assurance, audits, compliance and testing (37%) and cyber security research (36%)
- Around 1 in 5 cyber firms (18%) also say that job applicants lacking non-technical skills, such as communication, leadership or management skills, have prevented them from meeting their business goals. Around a quarter (23%) say this about their existing employees

Qualifications and training

Relevant technical training is still 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.

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

In the qualitative research, cyber sector firms discussed their approaches to training and skills development, and the challenges they faced:

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

It is still uncommon for businesses outside the cyber sector to provide cyber security training for wider staff. Just 1 in 10 (10%) have done so in the last 12 months and half (48%) of large businesses have done so. In the qualitative interviews, the cyber leads in these firms were eager for practical guidance on, and examples of, more effective training and awareness raising activities for wider staff.

Recruitment and staff retention

Almost half of cyber sector businesses (47%) have tried to recruit someone in a cyber role since the beginning of 2019. Of all the vacancies over this period, 37 per cent were reported as being hard to fill.

- The most common reason given for this continues to be around candidates lacking technical skills or knowledge (48% of employers with hard-to-fill vacancies), but mentions of job applicants lacking work experience have increased since the previous study (from 8% to 35%)
- In 3 in 10 cases (30%), cyber firms have found it hard to fill generalist roles (where employees are expected to work in a range of cyber security areas). The most common shortages in specialist roles are for senior management roles, penetration testing and security architecture

The secondary data analysis of online job vacancies focused on the latest calendar year (i.e. January to December 2020). Across all core cyber security job vacancies (i.e. where some aspect of cyber security is the main job function) posted over this more recent period:

- The most common roles in demand are security engineers (34%), security analysts (18%), security managers (14%), security architects (11%) and security consultants (7%)
- The sectors most in demand of cyber talent are the consultancy, finance and insurance, IT and cyber security sectors

- The technical skills areas most in demand are very consistent with the previous 3 years, and include skills around network engineering, risk management and technical controls, operating systems and virtualisation, cryptography and programming
- There are still geographic hotspots where demand is strongest, in cities like London, Leeds, Edinburgh, and Belfast, and across the West Midlands and the South West (in Bristol, Cheltenham and wider Gloucestershire)

The qualitative research uncovered several issues and challenges with recruiting cyber roles, from the perspective of both employers and recruitment agents:

- The organisations interviewed often held strongly negative views of recruitment agents and consequently favoured using networks and word-of-mouth recommendations to recruit. By contrast, recruitment agents pointed out that employers were often putting potentially unrealistic or unachievable criteria in job specifications, due to a lack of understanding of the labour market and the multitude of career pathways in cyber security. In these conversations, there was sometimes a lack of dialogue between recruitment agents, HR staff and hiring managers
- Organisations wanted candidates that exhibited more than just technical or soft skills. They were looking for innate qualities such as a willingness to learn, problem solving abilities and commitment

For the first time this year, the survey also explored staff retention. Across cyber sector firms, a total of 6 per cent of the cyber workforce are estimated to have left their posts since the start of 2019, with 4 per cent leaving of their own volition. Employers most commonly attribute this to a lack of pay or benefits. However, outside the cyber sector, the qualitative interviews highlight that a poor cyber security culture can also frequently drive people to leave cyber roles and look elsewhere.

Diversity

The cyber sector workforce continues to lack diversity relative to the rest of the digital sectors, and this is consistent when it comes to senior positions. Relatively few cyber firms have adapted their recruitment processes or carried out any specific activities to encourage applications from diverse groups.

- People from ethnic minority backgrounds make up 17 per cent of the sector workforce and 15 per cent of those in senior cyber roles (i.e. those typically requiring 6 or more years of experience)
- 16 per cent are female (vs. 28% across all digital sectors), with the same proportion in senior roles
- 10 per cent are neurodivergent, and this group makes up 8 per cent of those in senior roles
- 9 per cent are physically disabled, falling to 3 per cent in senior roles

The qualitative research highlighted various barriers and challenges when it comes to increasing workforce diversity in the cyber sector:

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

The impact of COVID-19

Online job postings for core cyber roles fell by around a third between March and April 2020, after the first COVID-19 lockdown. However, the volume of job postings had fully recovered to pre-lockdown levels by Autumn 2020.

In the qualitative interviews, we also explored the perceived impact of the COVID-19 pandemic:

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

Changes over time

This study builds on 2 previous waves, from 2018 and 2020. In general, the findings suggest the ongoing existence of cyber security skills gaps and skills shortages. Nevertheless, there is evidence of improvement in some areas, both in cyber sector businesses and the wider economy:

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

Conclusions

The latest cyber security labour market study reinforces many of the key messages from previous years. It also offers new insights on how UK organisations are meeting their cyber skills needs while dealing with the unpredictability of the COVID-19 pandemic. The main lessons are as follows:

- Across the private sector, it is still common to find skills gaps in basic technical areas, as well as more advanced areas. Cyber sector businesses are also grappling with niche technical skills gaps, hard-to-fill vacancies, and a need to build soft skills among their staff to help their business grow
- These issues are often exacerbated by perceptions gaps among key decision makers. This includes management boards and IT teams that lack an appreciation for cyber security, hiring

managers that may not be working as effectively as they could with HR staff and recruitment agents, and employers across all sectors who lack an understanding of workforce diversity

- There are also structural barriers, particularly for smaller cyber firms, who may find it hard implement structured training programmes, take on apprentices or other entry-level staff, and recruit outside of their relatively narrow existing networks
- Nevertheless, this remains a highly active and dynamic labour market, that has quickly recovered from an immediate post-pandemic drop in job vacancies. In fact, the changes brought about by COVID-19 raise new opportunities to engage senior managers on cyber security issues, look at innovative training solutions, and broaden recruitment practices to reach an enlarged talent pool

1 Introduction

1.1 About this research

The UK government Department for Digital, Culture, Media and Sport (DCMS) commissioned Ipsos MORI and Perspective Economics to conduct research to improve their understanding of the current UK cyber security skills labour market. It builds on two comparable research studies which Ipsos MORI conducted for DCMS, published in 2020 (also in partnership with Perspective Economics) and 2018.

The previous studies established that the UK, like other countries, has cyber security skills gaps (i.e. where existing employees or job applicants for cyber roles lack particular skills) and skills shortages (i.e. a shortfall in the number of skilled individuals working in or applying for cyber roles). This is part of a wider deficiency in digital skills, which the Employer Skills Survey 2019 found accounted for 38 per cent of all skills gaps – an increase from 35 per cent in the 2017 survey.

The 2021 research, in line with previous years, aimed to gather evidence on:

- Current cyber security skills gaps
- Current skills shortages and the level and type of job roles they affect
- 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
- Diversity within the cyber sector
- The role of training, recruitment and outsourcing to fill skills gaps

In addition, the 2021 research also had new research objectives and aimed to gather evidence on:

- Staff turnover in the cyber sector
- The role that recruitment agents play in the cyber security labour market

As in 2020 and 2018, the study also aims to create a set of recommendations, featured at the end of this report, on what the government and industry can do to tackle the cyber security skills gap.

1.2 Summary of the methodology

The methodology consisted of four strands:

1. **Quantitative surveys** – Ipsos MORI conducted representative telephone surveys with 4 audiences: general businesses, public sector organisations, charities and cyber firms. The cyber firms were sampled from a comprehensive list that had been compiled as part of DCMS's Cyber Security Sectoral Analysis 2021. These surveys gathered the main estimates on skills gaps and shortages reported in this study. Fieldwork was between 6 August and 30 October 2020.

2. **Qualitative interviews** – Ipsos MORI conducted a more focused strand of qualitative research, with 23 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 September and October 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 from September 2019 to the end of December 2020, supplementing the work done in the 2020 study (which covered vacancies from September 2016 to the end of August 2019).

4. **Recommendations workshop** – Ipsos MORI carried out a workshop with key stakeholders from government, industry and academia to discuss the findings from the preceding strands and contribute to the project's recommendations. This took place in November 2020.

1.3 Similarities and differences from the 2020 labour market study

Overall methodology changes and new audiences included in the research

The 2021 methodology is very consistent with previous years, which also included the four elements in Section 1.2. This allows both the survey and job vacancies analysis (the two quantitative elements) to look at trends over time. However, our approach deviates from previous years in the following ways:

- The 2018 and 2020 studies both included academic-led literature reviews to establish the existing evidence on cyber security skills gaps and shortages, and also to explore the approach that other countries outside the UK are taking to this issue (which is beyond the scope of the primary research). DCMS did not require a repeat literature review this year, as the evidence gathered in previous years was still considered relevant

- In 2020, we undertook qualitative interviews with UK cyber security training providers and did a review of training providers websites to understand the range of courses and formats being offered. This audience was not included this year, as the 2020 findings were still felt to be relevant

- The qualitative strand did not previously include recruitment agents – a new audience included for 2021. These interviews intended to explore the role of recruitment agents in the cyber security labour market in more depth. The same recruitment agent interviews also fed into a concurrent DCMS study on the cyber security recruitment pool, as the interview topics focused both on the demand side (in terms of employer demands and how employers work with agents) and the supply side (where agents found relevant job applicants and their own sense of the recruitment pool)

There is more detail on the rationale for changes across years in the separate technical report.

1.4 Differences from other well-known studies looking at cyber security skills

While we did not undertake a full literature review this year, the research team kept abreast of the major reports and statistics published in this area that covered the UK workforce, which helped to sense-check the findings from our research. These other studies include:

- Separate Ipsos MORI and Perspective Economics research for DCMS on the cyber security recruitment pool, which has also been published in 2021 and took place alongside this study
- DCMS's Cyber Security Sectoral Analysis 2021, which covers employment in the sector
- The Cybersecurity Workforce Study, which is an annual study by (ISC)^2, a global membership organisation for cyber security professionals, with the latest version published in 2020[1]
- The 2020 Cybersecurity Perception Study, also by (ISC)^2
- The DCMS Sectors Economic Estimates, particularly those for earnings and employment, which are annually published Official Statistics, covering the UK digital sector

[1] Before 2018, these were known as the Global Information Security Workforce Studies, or GISWS.

- The PwC Cyber Security Strategy 2021 report, which covered survey results with UK businesses and included a section on skills needs and hiring

The findings from the (ISC)^2 2020 report and the PwC Cyber Security Strategy touch on similar themes to our study (such as skills gaps, diversity in the cyber sector, qualifications and the impact of COVID-19) but they are not directly comparable to this research.

- 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 (ISC)^2 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

- 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 findings

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 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 2020 and 2018 study, this is indicating a statistically significant change over time.

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 MORI would like to thank the following partners who contributed at various stages to the study:

- Sam Donaldson, Perspective Economics
- David Crozier, Centre for Secure Information Technologies, Queen’s University Belfast
- Professor Steven Furnell, University of Nottingham

We would also like to thank the Cyber Security Skills and Professionalisation Team 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 and the qualifications they hold.

For context, in the survey of general (non-cyber) organisations, we asked participating organisations to choose the staff member most responsible for their cyber security to complete the survey. Just like in the 2018 and 2020 surveys, these individuals are not necessarily cyber professionals and the survey explores the extent to which such roles are formally labelled as cyber roles.

Key findings

- Almost half (45%) of businesses have just one employee responsible for cyber security. Large organisations tend to be slightly better resourced, typically with 4 to 5 people in cyber roles
- Within the cyber sector, half the cyber workforce (49%) entered their current role after working for another employer in a cyber role. By contrast, outside the sector, the staff performing cyber duties in-house are overwhelmingly transitioning from a non-cyber role (86%)
- A large proportion of non-cyber organisations have staff who carry out cyber functions doing so informally. Just 7 per cent of businesses have this role written into people's job descriptions
- By contrast, cyber sector employers appear increasingly to be professionalising these roles. A total of 70 per cent say that they have employees with, or working towards, cyber security-related qualifications or certifications (vs. 62% in 2020)

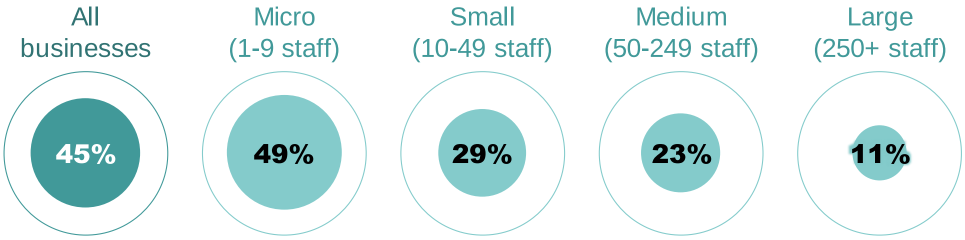
2.1 Size of cyber teams

Cyber teams outside the cyber sector

In-house cyber teams are typically very small. Almost half of businesses (45%) and two-fifths of charities (38%) have just 1 employee responsible for cyber security. Public sector organisations continue to be slightly better resourced in this regard, with a quarter (26%) having just 1 person in this role. These results are broadly in line with the 2020 survey.

As Figure 2.1 shows, larger organisations also tend to have slightly larger cyber teams. Among large businesses, the typical (median) cyber team comprises 4 to 5 people.

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



Bases: 965 businesses; 534 micro; 249 small; 117 medium; 65 large

These results are generally very consistent across sectors. The pattern of the data suggests that the finance or insurance, and information or communication sectors are often better resourced in terms of cyber security. The typical (median) cyber team in these businesses consists of 2 to 3 people.

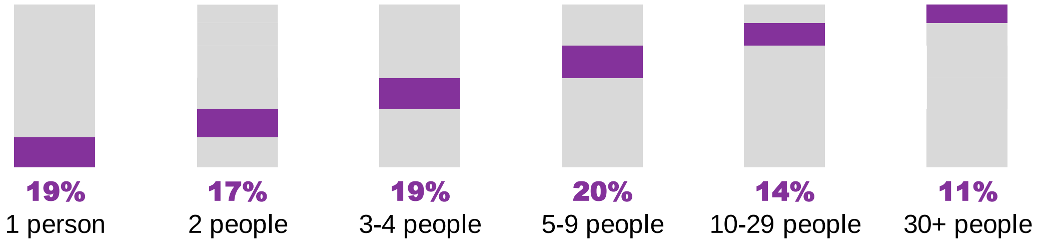
Those who outsource any aspects of cyber security are more likely to have more than one person in their in-house cyber team than those who do not outsource (58% vs. 47%). This suggests that outsourcing is more commonly used by organisations as a way of expanding their cyber capacity, rather than compensating for the absence of in-house cyber security staff. This was also the case in 2020.

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 latest DCMS Cyber Security Sectoral Analysis (2021) suggests this profile has remained consistent from 2020 to 2021 and estimates that 57 per cent are micro (1 to 9 staff) and 22 per cent are small (10 to 49 staff).

Our research finds that the typical (median) cyber team within cyber sector firms comprises between 3 and 4 people (Figure 2.2). These figures exclude people working in non-cyber roles in these businesses.

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



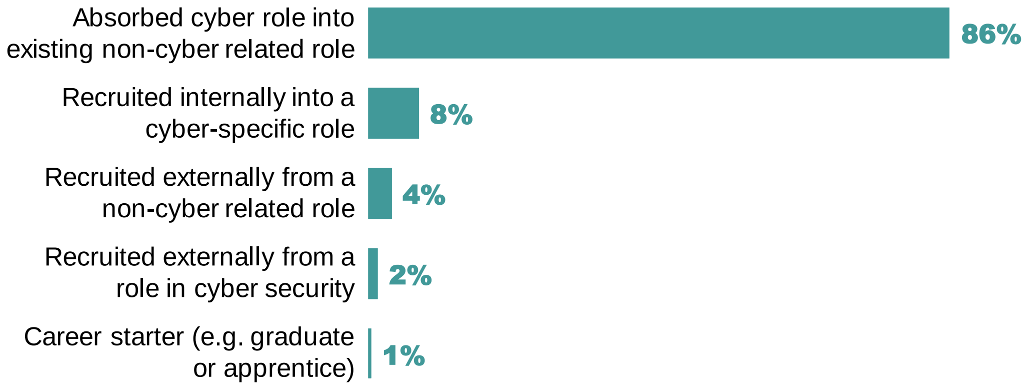
Base: 167 cyber sector businesses (i.e. excluding 4 from the full sample that did not provide this information)

2.2 Career pathways into cyber roles

Career pathways into cyber roles outside the cyber sector

Almost 9 in 10 of the staff carrying out any cyber functions in the private sector have absorbed these tasks into an existing non-cyber related role. 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. Just 2 per cent of the workforce entered their current role in this way. This suggests that organisations outside the cyber sector are relying overwhelmingly on upskilling and transitioning staff who may not have cyber-specific technical skills (e.g. IT staff) into cyber roles. Figure 2.3 shows the full data.

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



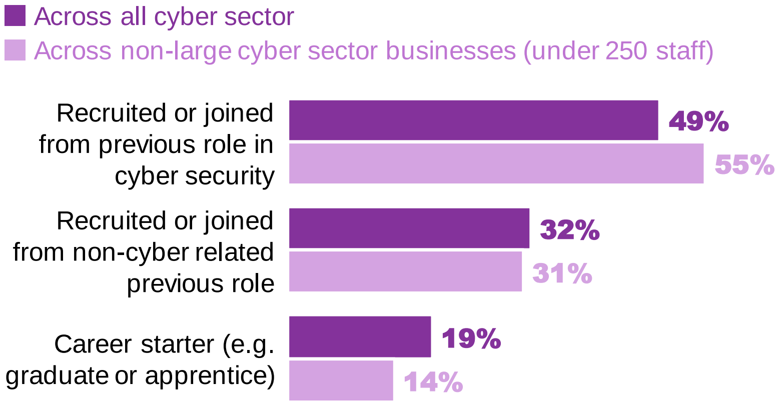
Bases: c.810 businesses (where answers given on team size and on how each individual came into the team)

Career pathways within the cyber sector

Within the cyber sector, half the cyber workforce entered their current role after working for another employer in a cyber role (49%). The other half have not come directly from a previous job in cyber security role (although they may still have worked on cyber security earlier in their careers). Within this half, it is more common for employers to take on those already in the labour market rather than career starters (32% vs. 19%). These statistics are very similar to the 2020 study.

As Figure 2.4 shows, the large firms in our sample skew this data considerably. When removing these firms (the light purple bars), fewer of the workforce have come in as career starters. This suggests that the large businesses in the cyber sector disproportionately take on graduates and apprentices, more so than smaller firms. This was also the case in 2020.

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



Bases: 156 cyber sector businesses (excluding those that could not break down their workforce); 153 non-large cyber sector businesses (under 250 staff)

Are internships or work placements offered in the cyber sector?

A third of cyber firms (28%) reported offering any internships or work placements since the start of 2019. This is a new question for the 2021 study.

The perceived benefits and challenges of hiring career starters

In the qualitative interviews, some firms had consciously moved towards a recruitment model that emphasised taking on entry-level staff and upskilling them, via apprenticeships (including degree apprenticeships) and internships, and had found this to be beneficial.

"We will take people straight out of university and train them up to be … cyber security people. We have had more success with that. That's playing the long game."

Cyber sector business

Individual interviewees mentioned the following rationale for this approach:

- A couple of cyber sector employers found that supposedly job-ready individuals would overstate their cyber security skills and knowledge in CVs and interviews, making it harder to filter candidates when recruiting beyond the entry level
- One cyber sector business noted that aiming for entry-level candidates had advantages in terms of long-term staff retention and not having to deal with high salary demands
- Another employer outside the cyber sector suggested that entry-level candidates with the right attitude could be more agile than candidates with experience, as they would not be tied to certain applications or ways of working from previous jobs

One of the recruitment agents also spoke of a more general trend towards work-based learning schemes across cyber employers, because these employers were increasingly valuing applied knowledge of cyber security above theoretical knowledge.

However, the interviews also suggest that there are ongoing barriers to taking on entry-level staff:

- Apprentices were sometimes strongly regarded as not being job ready, with too much time and resource required to bring them up to speed. One cyber sector business said that apprenticeships were too basic for their needs. Another suggested apprentices were, in their experience, not willing to carry out the non-glamorous work and put in the long hours that cyber roles might require

  "We have looked at apprenticeships in the past but have always found them to be set too low, the guys that are coming in on them are too inexperienced and there is too big a gap between where they are beginning from and where we need them to be."

  Cyber sector business

- Some felt they were simply too small to house career starters. Mirroring the findings from last year's study, we heard concerns about not having the time or resources to train apprentices

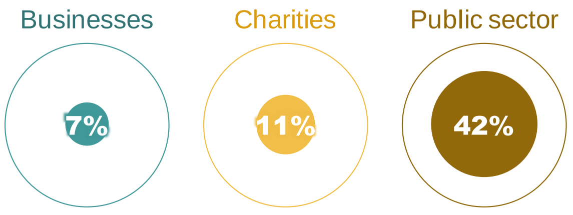
2.3 Are cyber roles labelled as such across UK organisations?

Both the previous studies, in 2018 and 2020, have found that a large proportion of organisations 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.

As Figure 2.5 shows, just 7 per cent of businesses have formalised the cyber role in this way in 2021. For public sector organisations, this is far more common (42%).

The finding for businesses marks a fall from 2018 and 2020, when it was 11 per cent.

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



Bases: 965 businesses; 220 charities; 76 public sector organisations

In the private sector, a higher proportion of medium (21%) and large businesses (26%) include cyber security in staff job descriptions. This is also more common in finance or insurance firms (29%) and information or communication firms (21%). Even amongst these sizes and sectors, the majority of businesses still do not have cyber security responsibilities as a formal part of their job descriptions.

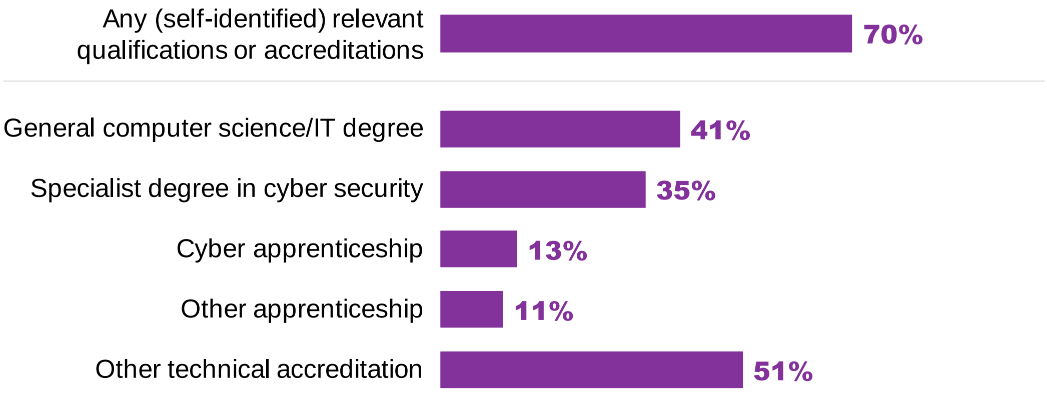
2.4 Qualifications of those in UK cyber sector firms

In this year's study we continue to focus on the qualifications of those in cyber sector firms as opposed to those working in other sectors. This is because, as covered in the previous section, cyber security across wider organisations is largely covered informally. 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.

A total of 7 in 10 cyber sector firms (70%) say that they have employees with, or working towards, a cyber security-related qualification or certified training. This is an increase from the 2020 study (when this was first asked), where around 6 in 10 (62%) said this.

Figure 2.6 highlights the kinds of qualifications or certifications that cyber firms say their staff have. Of note, these figures are based on <u>all</u> cyber firms, not just the 70 per cent that say their staff have any relevant qualifications or accreditations.

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



Base: 171 cyber sector firms

The most common types of higher education qualification that these firms identify are computer science or IT degrees, more so than cyber security-specific higher education qualifications (41% vs. 35%).

Nevertheless, both are less commonly mentioned than other technical accreditations (51%). While not explicitly covered in this year's survey, last year's results highlight that this includes a plethora of different accreditations, like Certified Information Systems Security Professional (CISSP) and others.

Last year, other technical accreditations also topped the list, which highlights that there is a great deal of emphasis in the cyber sector on cyber security-specific technical accreditations, over and above degrees or apprenticeships. Chapter 7 covers the specific types of technical accreditations that are most commonly mentioned in job postings, highlighting the extremely wide range of accreditations available in this sector.

In the qualitative research, we found that there are multiple drivers for taking employees through certified training. For one, offering these kinds of training and development opportunities came up in the recruitment agent and non-cyber business interviews as a way of attracting candidates.

In addition, some cyber sector interviewees said certification was a client requirement. One specifically saw this as a rising trend, evidenced by the fact that more of their clients were now stipulating proof of employee certifications in tenders and procurement frameworks. This might partly explain the increased emphasis on qualifications found in the cyber sector survey.

"We bid on a lot of frameworks and tenders and it is much more of a requirement now to show your technical capabilities in certification form, rather than just accepting that you have them because of the business you are in."

Cyber sector business

3 Diversity in cyber security

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

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 general businesses would provide a misleading picture of diversity in the cyber security labour market since the majority are performing cyber roles informally.

Key findings

- The cyber sector remains relatively nondiverse in terms of gender. Just 16 per cent of the workforce across these firms is female, compared to 28 per cent in other UK digital sectors
- Those filling senior roles (typically with 6 or more years of experience) are particularly nondiverse, across a range of characteristics including gender, ethnicity, disability and neurodiversity. For example, just 3 per cent of senior roles are filled by women
- Only a minority of cyber sector employers say they have adapted their recruitment processes to encourage these diverse groups to apply

3.1 Attitudes towards workforce diversity

The qualitative research suggests a low awareness of diversity as an issue to be grappled with in cyber security and a lack of consideration for the topic. Some of the cyber employers we spoke to admitted that they had not considered the issue at all before. This is a similar picture to last year's study.

> ***"It's not been something we've particularly thought about. We've had no positive programme to encourage or increase diversity. It has just organically formed the way it has. The best people come through the door really."***
> *Cyber sector business*

Different aspects of diversity also received different levels of consideration. Gender and ethnicity typically arose spontaneously when talking about this topic. There was widespread agreement that the cyber sector is male dominated, whereas the perceptions around ethnicity were far more mixed.

Ethnicity was sometimes conflated with nationality, for instance talking about having employees from Europe or elsewhere when asked about ethnicity. A lack of black minority employees was not specifically discussed, with some firms instead highlighting the strong presence of people of Indian origin in the labour market as examples of diversity.

Disability and neurodiversity were typically not on people's radars to the same extent. This was also the case in last year's study. Some were simply unaware of neurodiversity as a concept, and this needed

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

explaining in interviews. Some had never considered these groups specifically because they had not previously had any applications from them for cyber roles, or at least were not aware that they had.

Social class was also not typically on people’s radars. Some cyber leads felt it would be difficult or insensitive to ask about this during recruitment. One suggested you only got to know about people’s backgrounds once they had become employees.

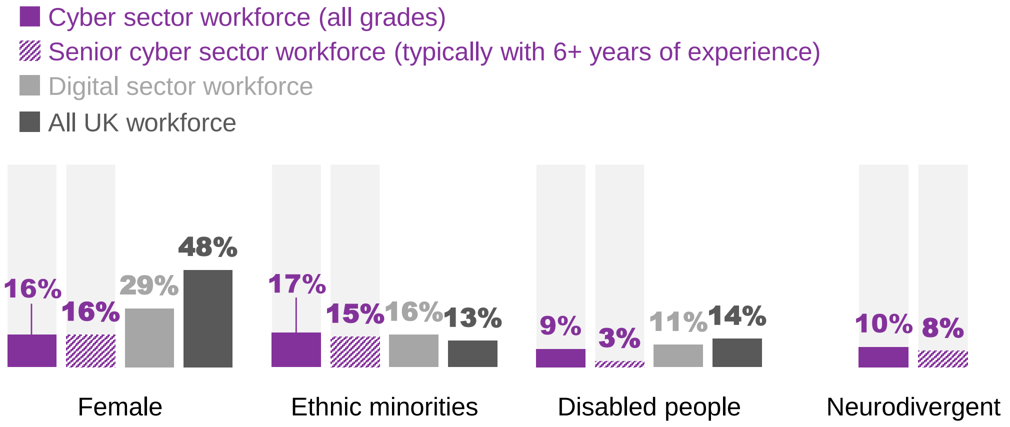
3.2 Estimates of diversity in the cyber sector

The quantitative findings in Figure 3.1 show that the cyber sector is behind other digital sectors with regards to gender diversity. It is more in line with other digital sectors when it comes to diversity of ethnicities and physical disability, although the latter is behind the wider UK workforce estimate.[3]

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). There are no reliable statistics to show how neurodiversity overall compares to other sectors.

These overall workforce diversity estimates are in line with the 2020 results. For the first time this year, the survey also collects diversity data for senior cyber professionals – that is, people who typically have 6 or more years of experience. As the chart shows, this more senior group exhibits a similar level of diversity to the overall cyber sector workforce across some of the characteristics measured, but not in terms of physical disability.

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



Bases: c.160 cyber sector businesses for all-grade workforce estimate; c.130 for senior workforce estimates (in each case excluding those that were not able to answer these questions, or refused)

3.3 Diversity in recruitment processes

Around half of cyber firms (47%) have tried to recruit people into cyber roles since January 2019 – our survey focused on activity over roughly the last 18 months before the interview. Among this group, only a minority report having adapted their recruitment processes or carrying out any specific activities to encourage applications from diverse groups. Specifically:

- A third of them (32%) say they made changes to recruit more women

[3] Gender, ethnicity and physical disability comparison data comes from DCMS Sector Economic Estimates: Employment Oct 2019–Sep 2020. This release covers a mixture of pre-pandemic and post-pandemic data.

- A quarter (25%) made changes for people from ethnic minority backgrounds
- One in five (19%) did so for physically disabled people
- Under one in five (15%) did so for people with neurodiverse conditions or learning disorders

There have been slight upwards shifts in some of these numbers since 2020, but the changes are not statistically significant.

3.4 Barriers preventing improvements in diversity

In the qualitative research, while cyber employers acknowledged that workforce diversity was an important issue and said they would be happy to recruit more diverse groups, they had often not taken any steps to influence this, for various reasons:

- It was commonly regarded as a difficult issue to tackle. A lack of applications from diverse groups was central to this perception. For example, when asked about neurodiversity, one cyber firm stated, “we haven’t discriminated … because we haven’t had anyone apply to consider.” There were similar opinions voiced about not getting female or ethnic minority candidates.

- Cyber employers often felt they could not influence who applied for jobs. On the other hand, some recruitment agents felt that hiring managers for cyber roles needed more educating on unconscious bias, best practice in writing unbiased job profiles and concepts such as blind recruitment. However, they did not feel it was their responsibility to impose these things, as ultimately this was the hiring manager’s decision

- Gender stereotyping was a problem. There was a perception among some employers and recruiters that women preferred less technical cyber roles, such as in communications or sales

- There was often a strong preference for recruiting via existing networks – which we discuss further in Chapter 6. This had negative implications for diversity. In the eyes of one cyber lead, everyone was recruiting from the same pool. Another mentioned recruiting a family member of one of their vendors. The implications could be more severe for senior roles, where some employers felt it was necessary to reduce risk by recruiting from networks

- Cyber employers putting an emphasis on the cultural fit of their employees could sometimes lead to diverse candidates being regarded as unsuitable. Recruitment agents felt this was especially a challenge for neurodiversity, as cyber employers would need to adapt their workplace culture to support neurodivergent staff and would need educating about this. One agent discussed this becoming a bigger problem over time, as neurodivergent staff could be considered socially awkward or lacking soft skills, which are increasingly sought after. Neurodiversity is explored in more detail in the separate DCMS research on the cyber security recruitment pool which discusses some of the challenges and ways to overcome these

- Unrealistic requirements within job adverts was a recurring theme. This was felt to hamper recruitment in general (which we cover in Chapter 6) but also impacted the diversity of recruitment. For example, one recruitment agent noted that women were less likely than men to apply if they did not match all the criteria mentioned in a job advert. Another agent noted that when they had put forward people from ethnic minority backgrounds, employers had wanted proof that the candidate was tried and tested. The theme of unrealistic requirements for women and ethnic minority candidates also came up in the separate DCMS research on the cyber security recruitment pool

- Some employers noted that finding ethnic minority candidates depended on the ethnic diversity of the local area. However, the qualitative research also found that, the shift to remote working that many firms had seen under COVID-19 had opened up opportunities for applicants from a wider geographical area. This may enable the recruitment of more diverse candidates in the future

- One business outside the cyber sector had tried to broaden their recruitment to include people without degrees, but this led to too many applications from people who lacked other basic skills, like being able to answer the telephone professionally, so they later abandoned this approach

- Where recruitment agents had been asked to diversify their candidate pools for cyber employers, this demand often came from HR leads rather than hiring managers. In one case, we heard that the HR lead had also helped to make job adverts more neutral. In other cases, hiring managers had not thought to ask their HR colleagues about this – one mentioned that their HR lead had complained about being involved at the last minute in recruitment requests. Moreover, smaller cyber firms often had no formal HR function, so lacked this voice entirely

  "The hiring manager will write what they are trying to do, and the talent team will take that and remove all of the male bias and other things, and make it appealing to a wider demographic."
  Cyber sector business

- There was also a lack of awareness of national initiatives to improve diversity within cyber security. Among the cyber sector firms that had heard of initiatives like CyberFirst and Cyber Discovery, there was a sense that these initiatives could be broader still in their recruitment. There were, however, mentions of other, often localised schemes, including Women in Cyber schemes, CodeClan and Black Codher, through which some cyber sector firms had recruited

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 (50%) of all private sector businesses identify a basic technical cyber security skills gap, i.e. a lack of confidence in performing a range of basic cyber security skills tasks or functions
- 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
- Around half of cyber sector firms (47%) have faced problems with technical cyber security skills gaps in the past 12 months, either among existing staff (18%) or among job applicants (40%)
- A total of 3 in 10 cyber sector firms (31%) have experienced a soft skills gap in this timeframe

4.1 Understanding of cyber security skills

Across all our qualitative research audiences, there was a sense that cyber security could be a very confusing area and that cyber security skills were, consequently, poorly understood and undervalued. Outside the cyber sector, this lack of understanding was apparent within management boards – one private sector interviewee was told when they were hired, “I don't know what you do, but I’ve been told I need you” – and also sometimes in IT teams. For example, one private sector cyber lead felt that their previous IT leadership lacked an understanding for how cyber security should permeate the business’s IT functions, so tended to underfund cyber security out of the IT budget and had avoided investing in training for the team. We spoke to another IT lead in the private sector who said any training they undertook at cost had to be linked to a specific IT project, and because cyber security cut across projects, it was typically overlooked when it came to training needs.

Senior managers sometimes underestimated the scale of tasks in cyber security. One interviewee recalled, for example, being asked to set up a cyber security framework, which senior management thought could be accomplished in 6 months, but ended up taking over 2 years.

Several factors exacerbated this lack of understanding:

- Outside the cyber sector, there was little appreciation of the multitude of cyber security career pathways and job roles. Employers often had unrealistic expectations for those in cyber roles to be experts across several areas such as information security, business continuity, data protection and business risk. One recruitment agent noted that job titles were often a poor indicator of actual job profiles – some titles, like Security Operations Manager or Information Security Consultant, could include a very different set of responsibilities in different firms. Another reported that it was a challenge to find generalist security consultants with both technical and compliance skills, because the balance of these skills that employers needed was often unclear

- There was not always a clear chain of command in cyber security, or enough knowledge across management boards, which could lead to a lack of ownership of the issue. One digital transformation manager in the public sector told us that their board assumed that the data protection officer, a different individual, was responsible for overseeing cyber security at a senior level. However, this person was overloaded with other, non-cyber work. It is worth noting that DCMS Cyber Security Breaches Survey series has also consistently highlighted the importance of board engagement with cyber security

> ***"There needs to be more visible ownership … It has been moved around quite a few times. It should be the whole board, not just one individual."***
> *Organisation outside the cyber sector*

Because cyber security was often not well understood or valued, staff in cyber roles could find themselves being pulled into non-cyber work in areas such as IT, business continuity and data protection. As one interviewee put it, a successful cyber security team would look like it is doing nothing, so other work could be pushed its way. They felt that an important part of any Chief Information Security Officer (CISO) role was to help protect and manage the resources of cyber teams, to maintain their focus on cyber security.

The impact of COVID-19

Outside the cyber sector, the COVID-19 pandemic had often brought cyber security to the fore. Among the organisations we interviewed, there was a very rapid shift to remote working which needed to happen at the same time as maintaining service continuity. The increase in remote working had accelerated certain IT changes, such as the move to cloud services, and created new cyber security threats. At the same time, higher threat levels in general were noted, for instance an increase in phishing attacks.

"There is no doubt that the threat level has gone up. Services are more pressurised. They are more focused on trying to deal with the demand that is placed on them. They are more fragile to an incident."
Organisation outside the cyber sector

In the short term, this had typically increased workloads and put more pressure on cyber teams, who had to implement new security controls and processes, and deal with new or elevated threats. We further discuss how COVID-19 has exacerbated skills shortages in Section 6.4.

However, it also presented an opportunity outside the cyber sector. Several cyber leads reported that cyber security had increased its internal profile, including with board members – one interviewee said they were now reporting directly to their management board for the first time – and some had taken advantage of this to argue successfully for extra investment in training and personnel for cyber teams.

"It's pushed the agenda right to the top. Remote working has made everyone move digital, so now senior management are taking notice of how important it is."
Organisation outside the cyber sector

This reflects a trend in the survey findings as well (covered in Section 4.7).

This was not, however, a universally positive impact in terms of investment in cyber security. As noted in Chapter 6, COVID-19 had also led to short-term recruitment freezes in some organisations.

4.2 Technical skills gaps outside the cyber sector

In line with previous labour market studies in 2018 and 2020, 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.

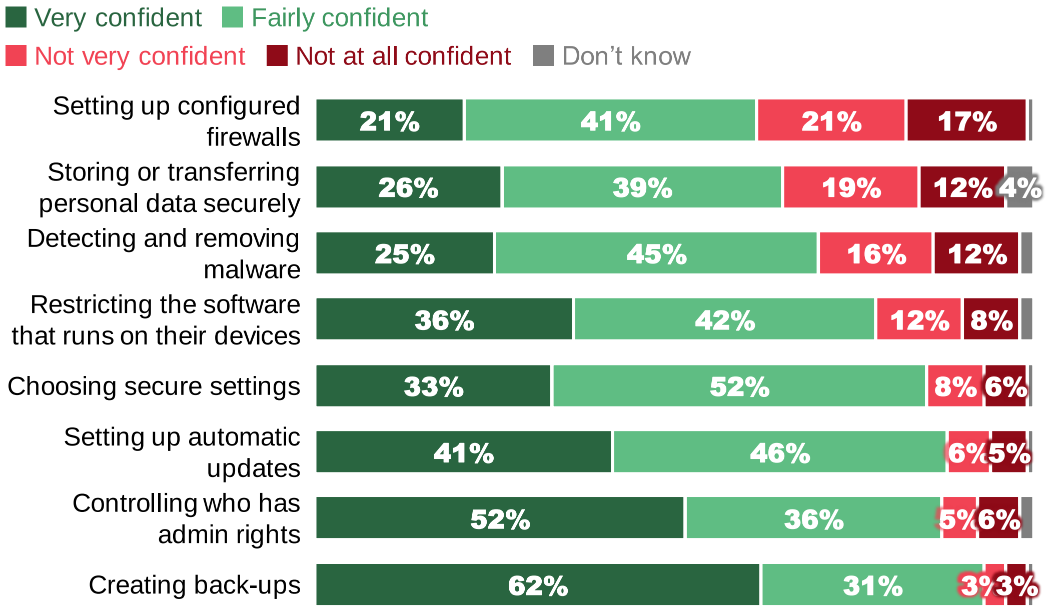
Where organisations outsource a cyber security task or function to external service providers, we do not count this as a skills gap. We cover the proportions outsourcing each task in Chapter 9.

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[4] 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 and detecting and removing malware, which is consistent with the 2018 and 2020 results. Nevertheless, only a minority of cyber leads across the business population say they are not confident in carrying out each of these tasks.

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



Bases: c.650+ businesses that do not outsource each task
Unlabelled bars are under 3%.

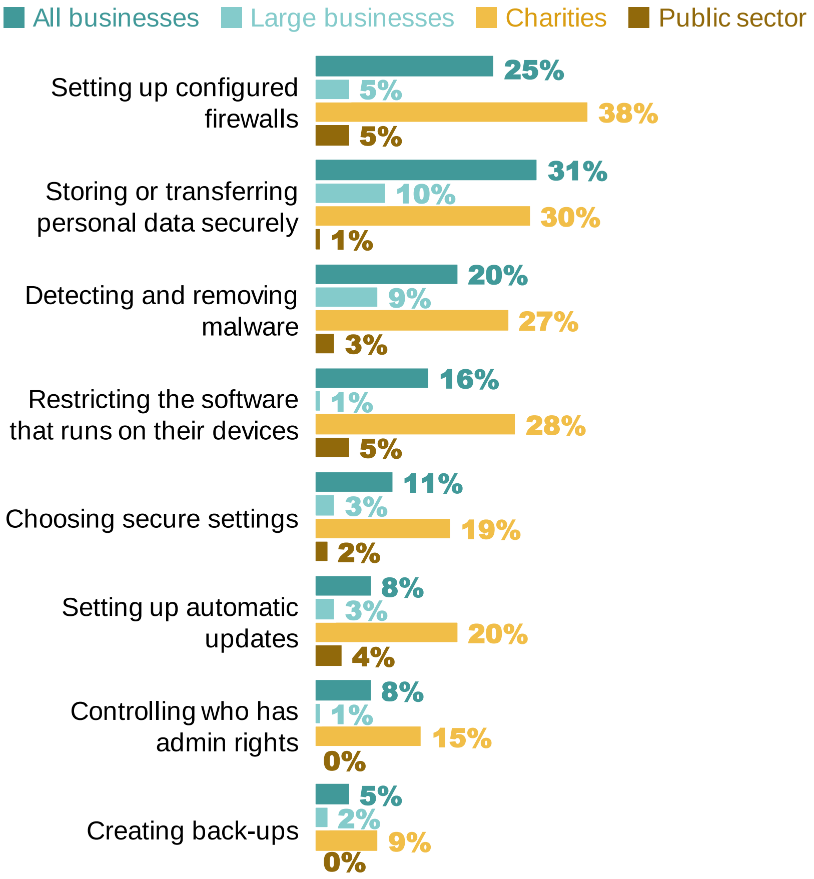
Figure 4.1 does not include businesses that outsource these tasks or functions, as by definition they do not need the skills to perform these tasks in-house. Figure 4.2 therefore rebases the proportion that are not confident out of all businesses (i.e. including the businesses that outsource cyber security in the

[4] 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).

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. On the other hand, charities are more likely than private sector businesses to have skills gaps in several areas, including setting up firewalls, restricting software, secure configurations (i.e. secure settings) and patch management (i.e. setting up automatic updates).

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



Bases: 965 businesses; 65 large businesses (with 250+ staff); 220 charities; 76 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.50+).

Across the 3 years of this study, skills gaps have fallen across several of these aspects of basic cyber security. Fewer are not confident in the following areas of cyber security compared to 2018:

- Setting up configured firewalls (25%, vs. 31% in 2018)
- Restricting the software that runs on their devices (16%, vs. 22% in 2018)
- Choosing secure settings (11%, vs. 16% in 2018)
- Setting up automatic updates (8%, vs. 15% in 2018)
- Controlling who has admin rights (8%, vs. 13% in 2018)
- Creating back-ups (5%, vs. 8% in 2018)

Information or communications businesses, and finance or insurance businesses continue to be among the least likely to identify basic skills gaps across this list of tasks. By contrast, basic technical skills gaps tend to be more prevalent among the construction sector. These sector differences were also present in the 2020 and 2018 labour market surveys.

A combined basic technical skills gap indicator

For a general sense of the number of organisations that have 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 50 per cent of businesses have a basic technical cyber security skills gap. This proportion is larger for charities (61%) and lower for public sector organisations (10%).

The basic cyber security skills gap is lower for large businesses (22%) and high-income charities (36% of those with £500,000 or more in annual income), although this still represents a sizeable minority of each group.

Extrapolating the overall business figure of 50 per cent to the overall population of private sector businesses, we estimate that approximately 680,000 businesses in the UK have a basic technical skills gap[5] as this is a representative survey based on the UK business population.

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:

- Only 44 per cent of those responsible for cyber security in the private sector and 37 per cent in charities say they understand the distinction between personal and boundary firewalls very well or fairly well. While most organisations may claim to feel confident at setting up configured firewalls, there is still a substantive knowledge gap around the basics of firewall management. In other words, this is likely to be a false sense of confidence in some cases. It suggests that our figures are a bare minimum estimate of the true basic skills gap

- Only a quarter in the private sector (24%) and around a fifth in charities (18%) say they understand what a sandboxed application is very or fairly well

There are no notable differences from the 2018 or 2020 results. The findings continue, therefore, to indicate a common lack of understanding across organisations.

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.

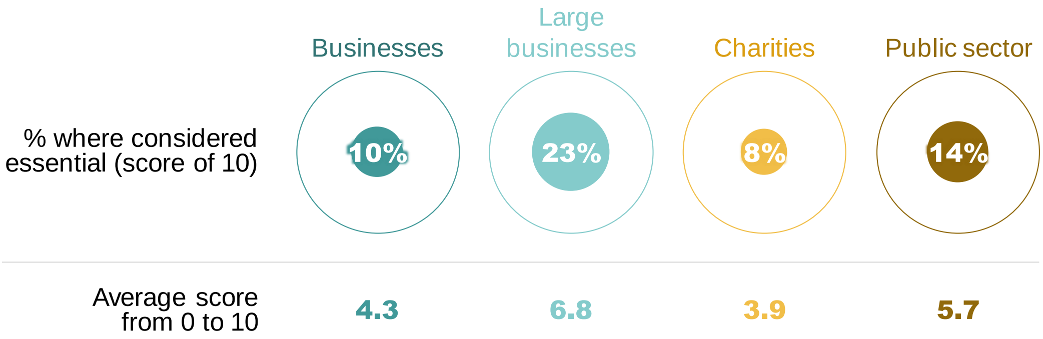
Our definition of advanced technical skills came about through the extensive scoping research carried out as part of the 2018 labour market study. It includes any skills associated with security architecture or

[5] The business population data is taken from the BEIS Business population estimates in 2020. These are the latest estimates 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 ±4.8 percentage points. This means that the true figure could be between approximately 615,000 and 746,000 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.

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 needs.

We asked organisations to rate how important it is for their cyber leads to have these 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 both previous years.

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



Bases: 965 businesses; 65 large businesses (with 250+ staff); 220 charities; 76 public sector organisations

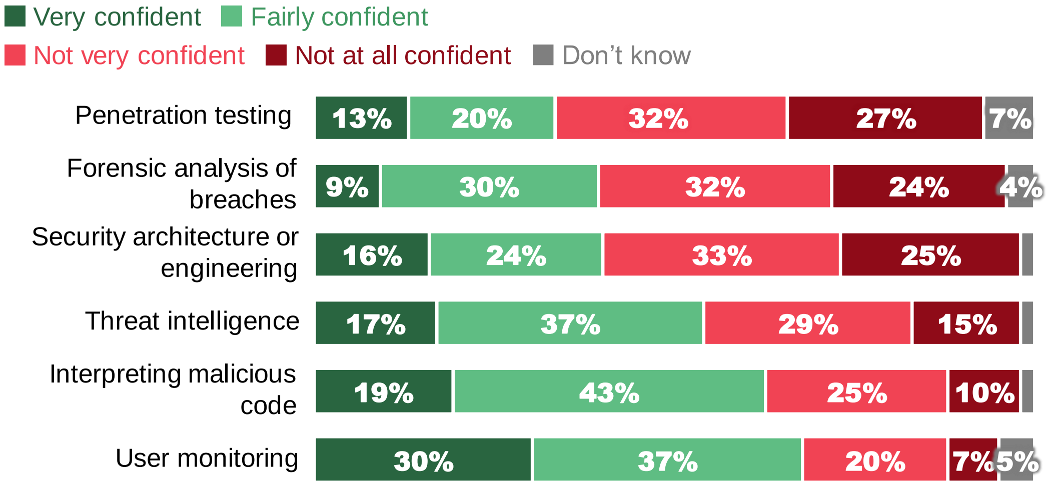
These advanced technical skills are considered to be more important among the information and communications sector (35%, vs. 10% overall).

Advanced technical skills gaps

Figure 4.4 illustrates businesses' advanced skills gaps, in the cases where businesses consider these skills to be important for their organisation[6] and do not outsource these areas of cyber security – i.e. in the cases where businesses have self-identified that they need these skills in-house. It suggests that advanced skills gaps are most prevalent when it comes to penetration testing, forensic analysis and security architecture or engineering. These results echo 2018 and 2020 findings, in which these 6 skills areas were ranked in the same order.

[6] 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).

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%.

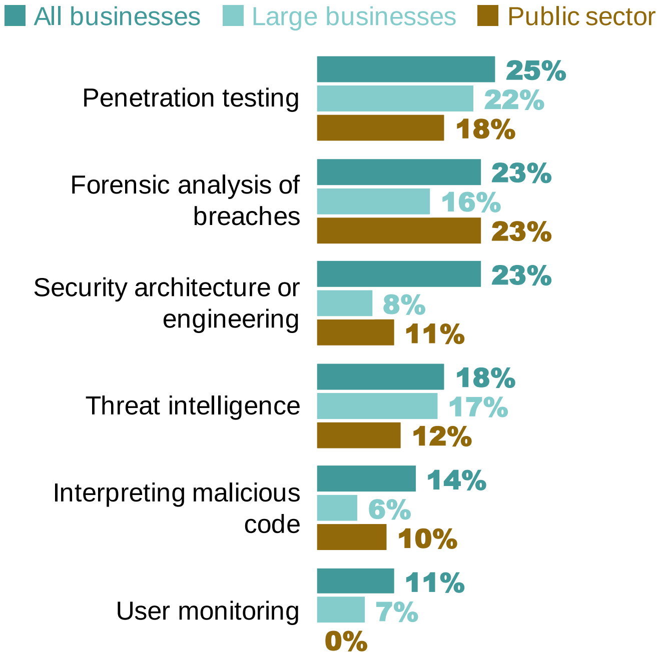
In Figure 4.5, we rebase these findings out of all businesses (including those that either outsource these tasks or do not consider them as important). This again gives a fuller picture of the proportion of the total population that has these advanced skills gaps. It also compares this to large businesses 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 advanced skills gaps tend to be similarly prevalent across different types of organisations, even different sized organisations. Once exception is security architecture and engineering, where skills gaps are greater among non-large businesses than large ones. This was also the case in 2020, and the findings are largely on par with previous years.

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



Bases: 965 businesses; 65 large businesses (with 250+ staff); 76 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.40).

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 340,000 businesses (25%) have a skills gap in penetration testing
- Around 313,000 (23%) have a skills gap in forensic analysis
- Around 313,000 (23%) have a skills gap in security architecture
- Around 245,000 (18%) have a skills gap in threat intelligence
- Around 191,000 (14%) have a skills gap in interpreting malicious code
- Around 150,000 (11%) 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 449,000 UK businesses. A quarter of charities also have an advanced skills gap (26%) – the lower result here reflects that fewer charities consider such skills to be necessary for their organisation compared to private sector businesses.

4.3 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 2021. 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 (18%) report having existing employees who lack necessary technical skills. Just 2 per cent say this prevents them meeting their business goals to a great extent, while 16 per cent say it does so to some extent.

By contrast, double this number of cyber firms (40%) say that the job applicants they have seen lack necessary technical skills. In total, 13 per cent say this is to a great extent, while 27 per cent say it is to some extent.

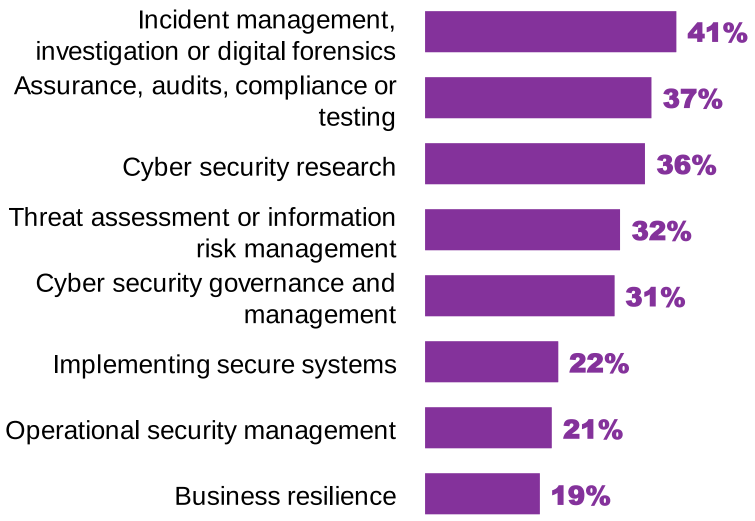
Both these figures have substantially declined since last year's survey. The technical skills gap measure has fallen by 14 percentage points for existing employees (from 32% in 2020) and by 19 percentage points for job applicants (from 59% in 2020). In both years, the question was framed consistently, 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 (47%) have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants. Again, this combined score is lower than in 2020 (when it was 64%).

Among this 47 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, formerly IISP) Skills Framework.

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



Base: 123 cyber sector businesses identifying any skills gaps

In summary, there is still an overall shortfall of specific skillsets, among which the largest gaps are in incident management and investigation, audits, and cyber security research. Skills gaps tend to be less prevalent for the bottom three categories: implementing secure systems, operational security management and business resilience.

Skills gaps are lower in three areas in comparison to 2020:

- Threat assessment and information risk management (32%, vs. 44% in 2020)
- Implementing secure systems (22% vs. 42%)
- Operational security management (21% vs. 34%)

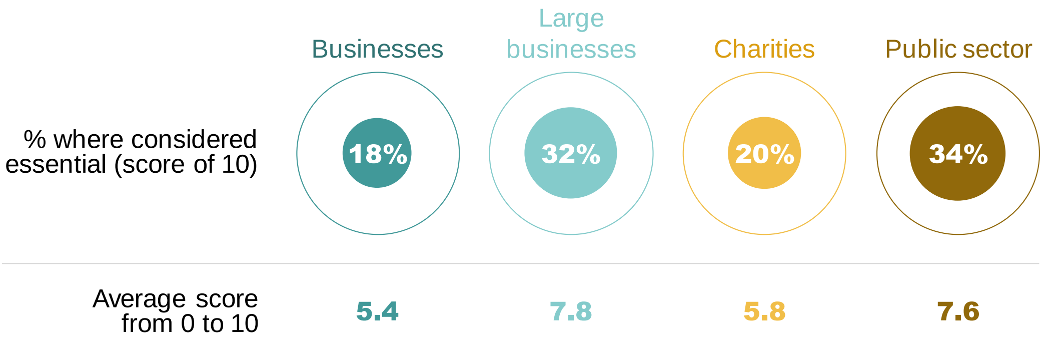
4.4 Incident response skills

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 (18%) of private sector organisations consider these skills to be essential, which rises to a third among large businesses and public sector organisations. This is similar to the 2018 and 2020 findings.

There is no difference in these results between the businesses that outsource cyber security and those that do not. In other words, even among those that would have to deal with any cyber security incident in-house, just a fifth consider it essential to have incident response skills among their staff.

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



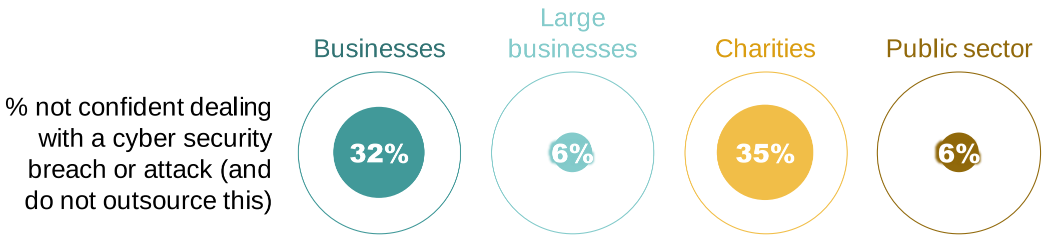
Bases: 965 businesses; 65 large businesses (with 250+ staff); 220 charities; 76 public sector organisations

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 38 per cent of businesses that outsource any aspect of cyber security, 82 per cent get their external cyber security provider to deal with incident response and recovery.

Among those that do not outsource this function, almost half of businesses (47%) 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 32 per cent of all UK businesses (when rebased to include those who outsource it) – shown in Figure 4.8.

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



Bases: 965 businesses; 65 large businesses (250+ staff); 220 charities; 76 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.40+).

Those in the construction (43%) and retail and wholesale sectors (42%) are both more likely than the average business (32%) to have an incident response skills gap in this way.

Almost half of all businesses (45%) are also not confident in their ability to write an incident response plan. A similar proportion of charities (44%) also say this. There are too few public sector organisations in the sample to report for this question.

4.5 Soft skills

The perceived importance of soft skills

The survey results show that cyber sector businesses are, by and large, aware of the importance of 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 score, is 8.3 out of 10. A third (34%) give the top answer of 10.

This question was not asked of organisations outside the cyber sector this year or last year. However, the data from the 2018 study suggests that cyber leads outside the cyber sector are equally aware of the importance of soft skills (30% gave the top answer in 2018, and the average score was 7.6 out of 10).

The qualitative research provides more nuance as to the kinds of soft skills being sought. Interviewees widely considered these to be an important part of the cyber security skillset.

- Strong communication skills were considered important to be able to relay technical issues to non-technical people, including board members (for organisations outside the cyber sector) or clients (for those in client-facing roles in cyber sector businesses). This included making business cases for cyber security infrastructure, budgets and resources, and explaining the implications of cyber security breaches. It also involved being able to discuss cyber security in terms of business risk, rather than using technical jargon

  "The only language they'll understand is money, so you need to show them what can happen if there is a breach."
  Organisation outside the cyber sector

- Outside the cyber sector, cyber leads needed to be able to influence behaviours and the culture among senior managers and wider staff. This required an understanding of human behaviour. One recruitment agent mentioned that they had seen a rise in cyber security awareness, training and culture roles in very large businesses, with recruits coming from previous roles in business analysis, psychology or sociology, rather than from technical computer science backgrounds

- Cyber sector businesses were looking for people with good interpersonal skills, as much of the work was done in teams rather than independently. As noted in Chapter 3, this could potentially conflict with the aim to have more neurodivergent individuals in cyber roles, as these individuals are often perceived to lack social skills

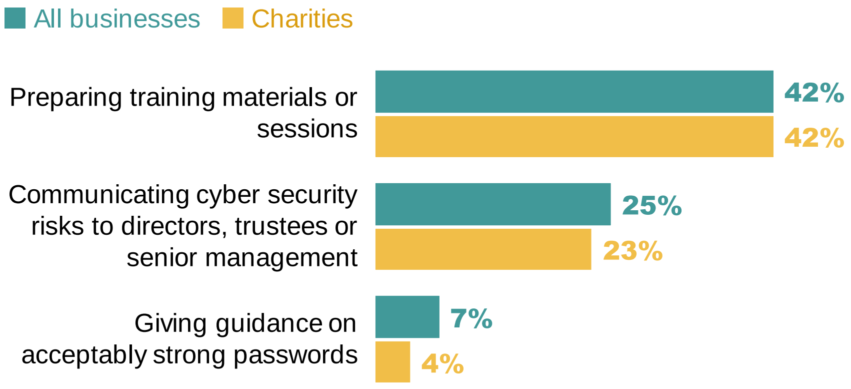
> ***"Cyber security is not one of those areas within tech that you typically associate with sitting on your own and coding … With cyber, you need that element of interpersonal skills as well."***
> *Recruitment agent*

- Cyber sector businesses were also seeking people with good client liaison skills, including the ability to present to clients and write proposals. This included people in sales roles, who needed a mix of technical understanding and commercial awareness. One interviewee said that they expected their sales staff to identify problems and pitch solutions with clients, before the more technically minded engineers got involved

Ability of cyber leads outside the cyber sector to undertake tasks mixing technical and soft 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 soft skills in order to be done successfully. Figure 4.9 illustrates the proportion of businesses and charities that have skills gaps in these areas. There are too few public sector organisations sampled to be reported for this question.

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



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

Cyber leads in the education sector (a mix of public and private sector organisations) are less confident than the average business (57%, vs. 42% not confident overall), in preparing training materials or training sessions for staff who are not specialists in cyber security.

Do cyber sector firms identify a soft 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 2021 (which used a comparable methodology). They are reported here for the first time.

Around 1 in 5 cyber firms (18%) say that, over the last 12 months, they have seen job applicants for cyber roles lacking communication, leadership or management skills. A total of 4 per cent say has stopped them meeting their business goals to a great extent while 14 per cent say this is to some extent. The 18 per cent result is down from 2020 (when it was 29%), indicating that soft skills gaps have become less of an issue.

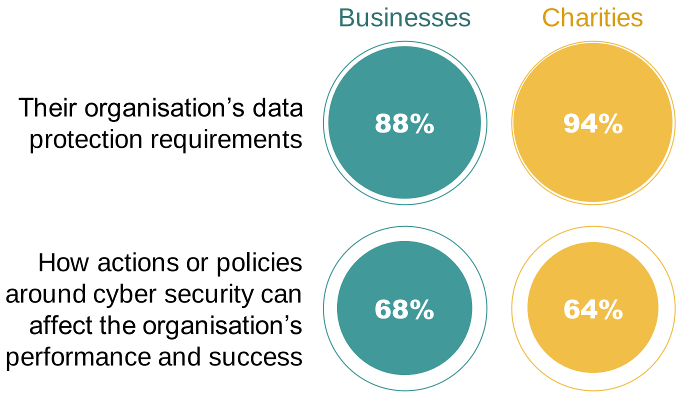
Around a quarter (23%) say that their existing employees lack these soft skills (with 3% saying this impacts them to a great extent and 21% to some extent). This figure has also decreased from the 2020 score, although in this case the change is not statistically significant.

When combining these scores for existing staff and job applicants lacking soft skills, the result is that 31 per cent of cyber sector employers have experienced a soft skills gap in the previous 12 months. Comparing this to the results on technical skills gaps in Section 4.3 (where 47% say they have experienced technical skills gaps) suggests that a lack of soft skills remains an important issue but is less substantial than the technical skills gap.

4.6 Governance and compliance skills

Those in cyber roles frequently need strategic management skills to perform their role effectively, particularly in governance, regulation 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. At the same time, around a third admit to being uncertain about how cyber security could affect business performance. 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

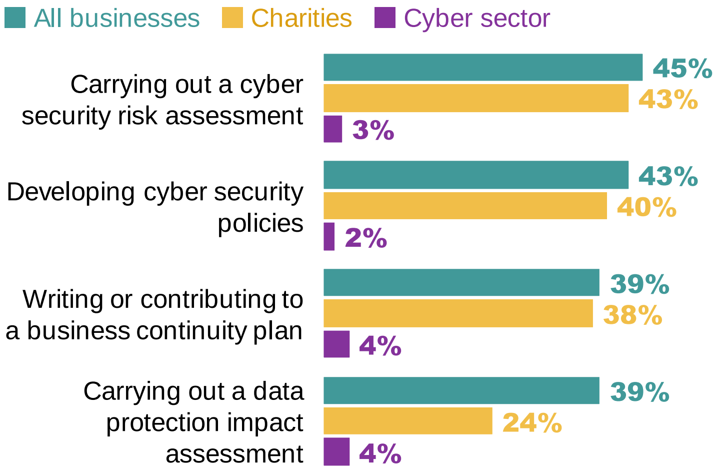


Bases (asked to a random half of full sample): c.470 businesses; c.100 charities

And when it comes to being able to carry out cyber security governance tasks, there are widespread self-identified skills gaps. As Figure 4.11 suggests, almost half (45%) of private sector cyber leads are not confident in their ability to carry out a cyber security risk assessment. Around 4 in 10 also lack confidence in developing cyber security policies, writing business continuity plans, and carrying out data protection impact assessments. Charities are mostly in line with businesses but tend to be more confident when it comes to writing data protection impact assessments.

These findings are, again, in line with both 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.80 cyber sector businesses

We also ask these questions of cyber sector businesses. They continue to be overwhelmingly confident at being able to carry out these tasks for their own organisations.

Elsewhere in the survey, we establish the perceived importance of this broader GRC knowledge among cyber sector employers. Half (51%) say it is essential for their staff to have an understanding of the legal or compliance issues affecting cyber security, indicating that skills needs typically go beyond both technical and soft skills.

4.7 Cyber security skills gaps in the non-cyber workforce

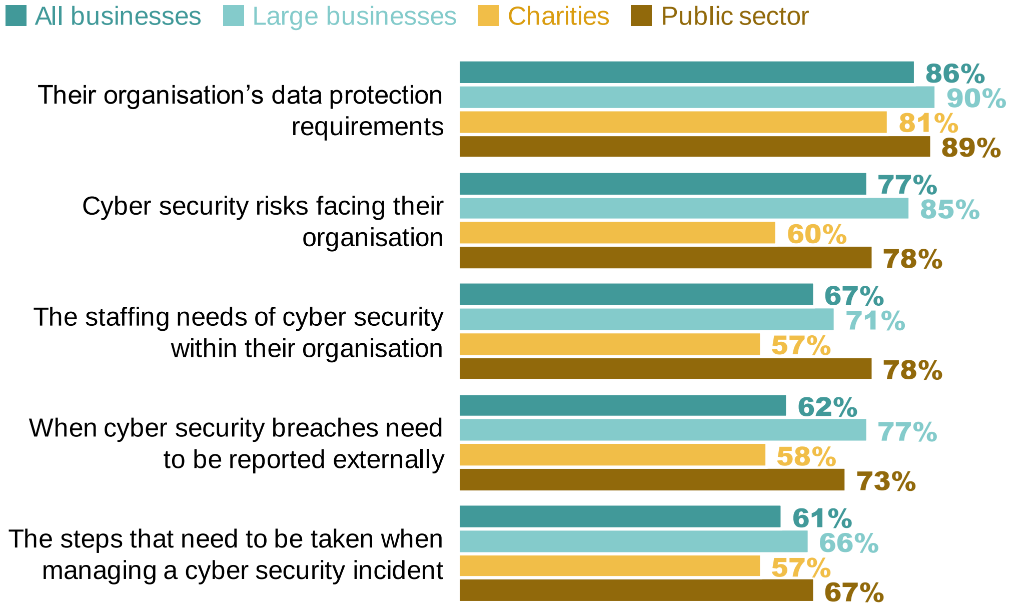
Senior managers and wider staff outside of cyber teams also needed to have the right skills and knowledge to be able to understand and interpret cyber risks, recognise their GRC responsibilities, and follow the cyber security rules and processes set by their organisation. This section explores skills 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 senior managers do not understand the staffing needs of cyber security within their organisation.

These results have improved over time. Within businesses, the proportion that say that their senior managers understand the cyber security risks facing their organisation has risen from 62 per cent in 2018, to 70 per cent in 2020 and 77 per cent this year. The proportion saying that they understand the staffing needs of cyber security (59% in 2018) and how to manage a cyber incident (59% in 2020) rose from 2018 to 2020, and in each case, this rise has been sustained in 2021.

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: 965 businesses; 65 large businesses (with 250+ staff); 220 charities; 76 public sector organisations

Across these indicators, management boards tend to be more highly rated in the finance and insurance sector, and information and communications sector. Cyber leads in the health, social work and social care sector (74%) and education sector (72%) also tend to be more certain about senior management knowledge around breach reporting than in the average firm (62%). Those in the health, social work and social care sector are also more certain that senior managers know the steps to take following a cyber incident (77%, vs. 61% across all businesses).

As discussed in Section 4.1, a lack of understanding of cyber security among senior staff, both at the board level and within IT teams (outside the cyber sector), was a key issue raised in the qualitative research. While the survey trends suggest things have improved over time, the qualitative findings highlight an ongoing tension between cyber leads and senior managers, potentially based on cyber security not being considered in terms of business risk, and therefore being undervalued.

Where cyber security was not valued at a senior level, this was seen to have a trickledown effect on the rest of the organisation, leading to a poor cyber security culture among wider staff and a lack of investment in cyber security skills and training. For example, one interviewee linked the attitudes of senior managers to their wider staff training on cyber security not being mandatory, and to staff not being sanctioned when they did not meet cyber security requirements. This again mirrors findings from the DCMS Cyber Security Breaches Survey series.

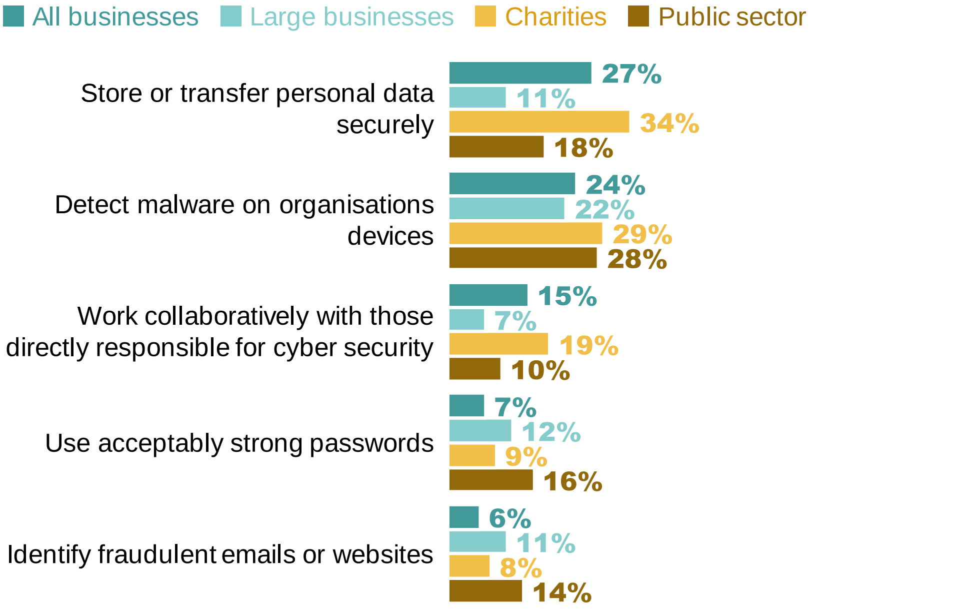
Cyber security skills among wider staff

When looking at the wider staff across all businesses (i.e. not in-house cyber teams or board-level staff), cyber leads are generally 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. 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.

These results are in line with the 2020 findings. The proportion that are confident in their core staff being able to store and transfer personal data securely remains higher than in 2018 (when it was 58%, vs. 67% in 2021), which suggests a lasting impact from the General Data Protection Regulation (GDPR), which came into force 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: 965 businesses; 65 large businesses (with 250+ staff); 201 charities; 76 public sector organisations

Across each of these indicators, those in information and communications businesses tend to be more confident than average about their wider staff acting appropriately when it comes to cyber security.

4.8 Upcoming skills needs and challenges

The qualitative interviews explored how cyber skills needs might change in the next 3 to 5 years. In these discussions, we identified various potential trends:

- Roles would continue to become more specialised and fragmented, with, for example, existing roles and job titles, becoming cloud-related – security engineers becoming cloud security engineers. This raises the possibility of the labour market becoming more complex and confusing
- There is growing automation in cyber security. One interviewee highlighted that this raises challenges for future cohorts entering cyber roles, as the baseline requirements will increase, and they may not have as many opportunities to develop their skills in junior roles

> ***"Part of the problem is that the entry point for cyber roles is going up. You have to become more and more skilled to get a foot on the ladder. A lot of technology solutions are replacing some of those entry roles."***
>
> *Cyber sector business*

- Another implication of increasing automation is that the required skills base in various cyber roles may evolve and shift away from more traditional software engineering towards data analysis. Data analytics skills will be increasingly needed to drill down into any issues identified by automated processes – something also acknowledged in the DCMS National Data Strategy (2020)

- Specific skills areas were mentioned as being likely to grow in importance. These included cloud security and artificial intelligence (which both came up in last year's study), skills around awareness raising and training and DevSecOps (the security aspect of DevOps). The specialist skills cyber sector firms wanted to develop were closely tied to the products and services they offered. From this perspective, some interviewees talked about relatively niche skillsets, including one-off mentions of blockchain technology, biometrics and specific programming languages

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

- Three-fifths of cyber sector businesses (60%) report having undertaken a cyber security training needs analysis in the past year (up from 49% in 2020). Just a fifth of businesses outside the cyber sector (18%) have done so
- The number of cyber sector firms saying that staff in cyber roles have undertaken training relevant to their roles has increased (from 73% in 2020 to 79% in 2021). Among businesses, this has not changed and remains around a quarter (23%)
- Just 1 in 10 businesses (10%) have provided cyber security training to non-cyber staff. In two-thirds of cases (66%), this training specifically covers home working or use of personal devices

5.1 Training needs

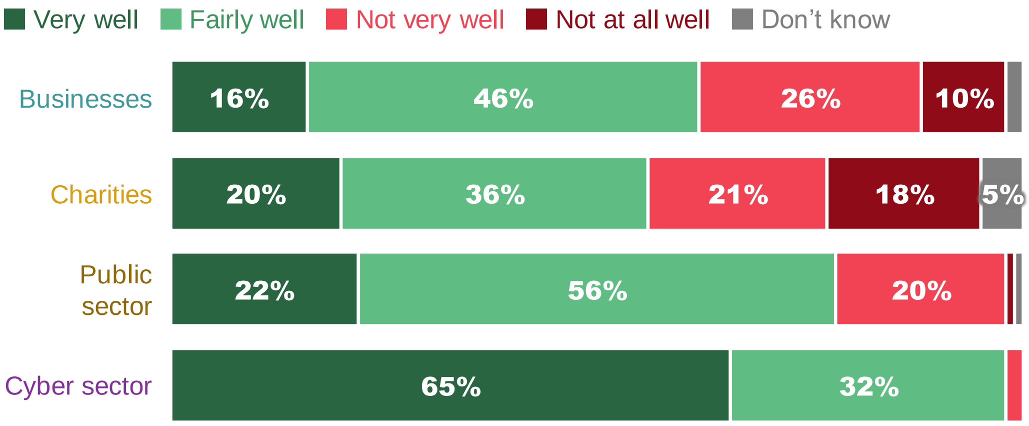
How well organisations feel they understand their training needs

Most organisations feel they understand their cyber security training needs at least fairly well – three-fifths of businesses (62%) say this – but few outside the cyber sector say they understand these needs *very* well, as Figure 5.1 shows. Charities are almost twice as likely as businesses to say they understand their training needs *not at all well* (18% vs. 10%).

In the case of cyber sector businesses, two-thirds (65%) feel they understand their training needs very well. As in the 2020 survey, this still leaves around a third that do not pick this top answer, suggesting there is still room for development.

Across all these groups, the findings are broadly level with those from 2020 (when this was first asked).

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



Bases: 965 businesses; 220 charities; 76 public sector organisations; 171 cyber sector businesses
Unlabelled bars are under 3%.

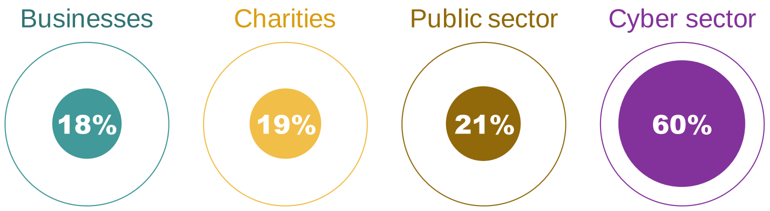
Information and communications businesses are more likely than average to say they understand their cyber security training needs *very* well (35%, vs. 16% overall). Large businesses also tend to report a better understanding of their training needs, with 3 in 10 (29%) saying they understand them very well.

Formally analysing training needs

The self-reported understanding of training needs can be contrasted against the proportion that have undertaken a formal training needs analysis. As Figure 5.2 shows, just a fifth businesses and charities have done this within the past year.

The business and charity results are consistent with previous years. For public sector organisations, the proportion has fallen since 2020 (from 44% to 21%). For cyber sector firms, however, the results have improved this year – the number that have undertaken a training needs analysis is 11 percentage points higher than in 2020 (when it was 49%).

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



Bases: 965 businesses; 220 charities; 76 public sector organisations; 171 cyber sector businesses

The following sectors are more likely than average to have undertaken such an analysis:

- Finance and insurance (45%, vs. 18% overall)
- Information and communications (29%)
- Health, social care and social work (27%)

5.2 Training undertaken by those in cyber roles

A quarter of businesses (23%) report having any of their staff in cyber roles undertake training relevant to their roles in the last year. The proportion is the same for charities (23%) and higher among public sector organisations (44%). As might be expected, cyber sector firms report the highest amount of training undertaken (79%).

The trend over time again differs across groups. For businesses and charities, the results are in line with 2020 (when this was first asked). Fewer public sector organisations had staff in cyber roles trained this year (down from 66% in 2020). By contrast, the number of cyber sector firms training staff has increased by 6 percentage points (from 73% in 2020). This aligns with the earlier finding (in Section 2.4) that more cyber sector firms have staff with or working towards cyber security qualifications than in 2020.

Businesses in the following sectors are more likely than average to have had cyber security staff undertaking training:

- Information and communications (51% vs. 23% overall)
- Finance and insurance (50%)
- Health, social care and social work (37%)

- Education (36%)

It is also far more likely for medium (46%) and large businesses (47%) to provide such training than the average business.

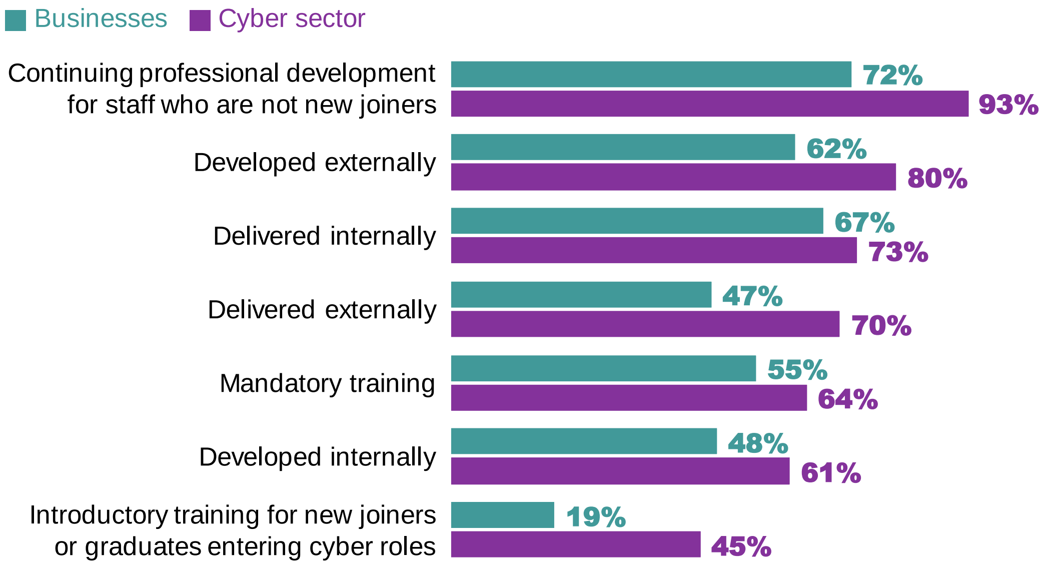
Features of the training being undertaken

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. The pattern of findings is similar for charities and public sector organisations, but the samples for these groups are too small to report for this question.

The results highlight that training is more commonly directed at established cyber security staff rather than career starters in these roles, both within and outside the cyber sector. It also suggests that, where organisations are providing training for those in cyber roles, they 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.

These results are largely consistent with the 2020 survey (when they were first collected). However, one notable change in the case of cyber sector firms is that fewer are providing training for career starters (down from 63% in 2020 to 45% now, among those where any cyber staff are undertaking training).

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



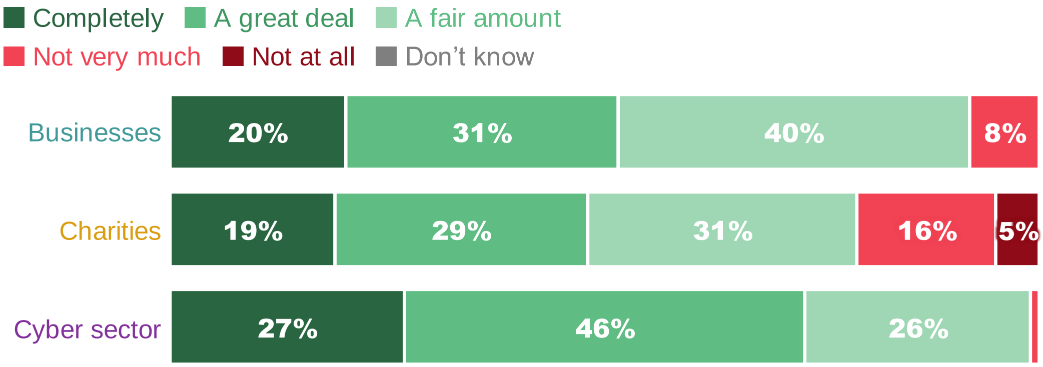
Bases: 313 businesses that have had staff in cyber roles undertake training; 135 cyber firms that have had staff in cyber roles undertake training

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. However, there is generally less confidence in the training being fit for purpose outside the cyber sector – around 5 in 10 businesses say the training only met their needs *a fair amount* or *not very much*. And 5 per cent of charities say the training did not meet the needs of this group of staff at all.

For all organisations, these results are broadly consistent with those from 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): 313 businesses; 68 charities; 135 cyber sector businesses
Unlabelled bars are under 3%.

5.3 Approaches taken to training those in cyber roles

In the qualitative interviews, we explored what approaches cyber leads had taken for their own training and skills development and that of their teams.

Larger firms often had structured career development programmes, which were felt to help with staff retention. For instance, one large cyber firm has a 6-month entry-level program, with the first 3 months being mostly full-time study, before trainees moved on to do shadow engagements for clients. This firm had retention periods of 4 to 7 years, so felt this approach paid dividends.

Some cyber firms also provided labs and test networks, where junior staff could experiment in a safe environment where mistakes do not matter, before working directly with clients. These were seen as an effective way to learn through practical experience.

Structured programmes were less common in smaller firms. Therefore, they relied much more on on-the-job training, work shadowing and mentoring schemes to disseminate knowledge and skills.

Self-directed learning was also important in these smaller cyber sector firms. One interviewee discussed how one of their senior staff would become a self-taught expert on a new product or technology and then take responsibility for informally training the rest of the team. In a similar way, outside the cyber sector, one interviewee mentioned using the free Open University courses on cyber security. These themes also came up in last year's study.

The smaller cyber sector businesses were typically very conscious about getting value for money from external training. Another interviewee noted that if they ever had anyone sent on an external training course, this individual was then expected to share their learnings across the team.

The interviews also explored the use of existing knowledge and skills frameworks in training. Most of those we spoke to said they did not use frameworks for training. The main reason given was that frameworks were not considered relevant when the business specialised in a particular area of cyber security. In these instances, a general cyber security skills framework could be too broad.

5.4 Gaps in training and training barriers for those in cyber roles

Gaps in non-cyber sector organisations

In the qualitative research, organisations outside the cyber sector identified two key gaps in the current training available:

- Influencing senior management on cyber security
- Effective ways to promote cyber awareness among employees

As discussed in Chapter 4, senior management not valuing cyber security was a source of frustration for cyber team heads. It was thought that training or guidance for cyber leads on how to influence senior management, helping them to understand the importance of cyber security and what steps need to be taken to protect organisations, would be valuable.

"We get it, but we don't think they get it. How do you break those barriers down to get the board engaged and to support the board in that engagement?"

Organisation outside the cyber sector

There were some concerns about the current training in their organisations amounting to annual box ticking exercises, which did not necessarily instil good habits. These cyber leads were, consequently, eager for practical guidance on, and examples of, more effective training and awareness raising activities for wider staff – they felt this was a gap in their own knowledge and skills.

"Deliver us some more effective tools in terms of promotion on the ground that would bring people's awareness levels up."

Organisation outside the cyber sector

There was also one example of a firm where the cyber lead had a poor understanding of training pathways to help their IT staff build cyber security skills. After doing their own research online, they had started to put team members on courses for the Certified Information Systems Security Professional (CISSP) accreditation, among others. This is despite CISSP being a very broad qualification covering multiple areas of cyber security. This solitary example suggests there may be value in promoting more efficient training pathways for transitioning IT staff.

Gaps within the cyber sector

The two areas where training gaps were mentioned in cyber sector interviews were in soft skills development and in niche technical areas related to their product or service offering. One interviewee said that none of the training they had tried had worked especially well at building soft skills, such as presentation and proposal writing skills. However, relative to those outside the cyber sector, the cyber firms we spoke to were not particularly concerned about gaps in the training available to them.

5.5 Cyber security training or awareness raising activities for wider staff

Overall, 1 in 10 businesses (10%) and a similar proportion of charities (12%) 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 (28%) and large businesses (48%). Public sector organisations are also much closer to larger businesses in this regard, with 4 in 10 (40%) having provided this kind of training.

Cyber security training for wider staff is more prevalent in the finance and insurance sector (29%) and information and communications sector (28%).

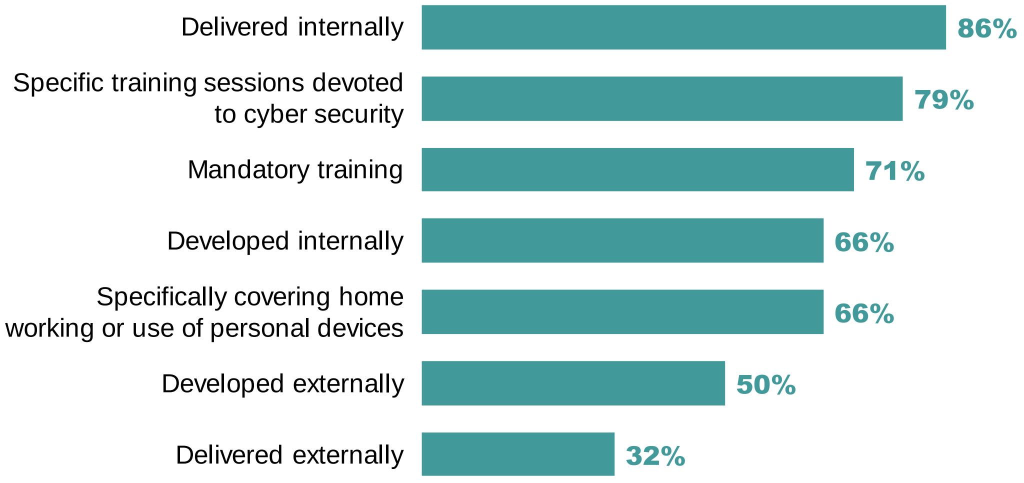
These findings (overall and sector subgroups) are very similar to the 2020 survey.

Features of the training being undertaken with wider staff

As Figure 5.5 shows, these training sessions are more likely to be both developed and delivered internally rather than externally, in contrast to training sessions 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 (79%). They are also more likely to be mandatory than training sessions for those in cyber roles (71%, vs. 55% for those in cyber roles in the wider private sector).

This year, we asked for the first time whether training covers home working or use of personal devices. This is in light of the COVID-19 pandemic and associated restrictions across the UK, which have led to many employees working from home. In two-thirds (66%) of cases, businesses report that their training does cover these aspects.

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



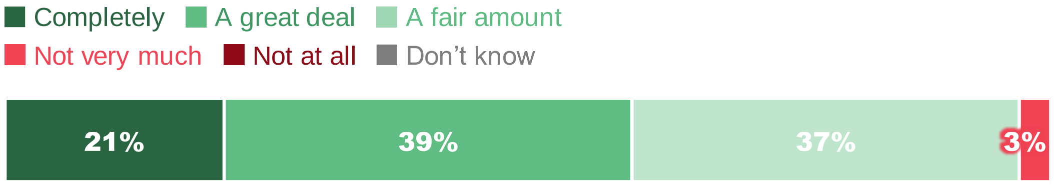
Base: 180 businesses that have undertaken training or awareness raising sessions for non-specialist staff

Perceived effectiveness of training for wider staff

The survey found that 3 in 5 businesses (60%) think that any cyber security training for wider staff met the needs of the organisation *a great deal* or *completely*. The sample sizes for charities and public sector organisations are too low to report this question.

Again, these results are broadly consistent with those from 2020.

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



Base: 179 businesses that have undertaken training or awareness raising sessions for non-specialist staff

What makes for effective training for wider staff?

As noted earlier in this chapter, in the qualitative research, firms outside the cyber sector were clamouring for more guidance on the kinds of training and awareness raising activities that would have the most impact on their wider staff.

When discussing cyber security training for wider staff, cyber leads outside the cyber sector commonly considered the more interactive and practical training activities to be the most impactful. One interviewee discussed the power of being able to demonstrate what phishing emails today can look like and how complex they have become. Mock phishing exercises were also considered especially effective.

Another interviewee felt it would be useful to have a quiz attached to their existing all-staff training. On this note, the National Cyber Security Centre (NCSC) does have a Stay Safe Online free training package and knowledge quiz, and it may be worth promoting this more widely to UK organisations.

5.6 The impact of COVID-19 on training

The qualitative research found that the pandemic had impacted training in two ways:

- Invariably, organisations had been forced to make all their training virtual (both for those in cyber roles and for wider staff). This raised challenges around replicating classroom environments. One interviewee outside the cyber sector felt staff were less easily engaged with virtual training. However, one cyber firm, which had moved training online before the pandemic, noted that this format was also more flexible, as it saved their staff having to make a 3-day trip to London

- Shadowing on the job was seen to be harder in a virtual environment

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. While we asked the same questions in the 2020 survey, that survey covered any job vacancies over a 3-year period (roughly up to the start of 2017). We now focus on a different timeframe – job vacancies since the start of 2019 – to remove any overlap with the data from the previous survey. This report still draws comparisons between the 2 years' results, but it should be noted that the baseline results from 2020 reflect the entire 3 years prior.

The qualitative data is broader, as it covers the 3 groups that we interviewed: cyber sector businesses, other the medium and large businesses outside the cyber sector, and recruitment agents who recruited cyber security roles. This strand of the research also explored how recruitment approaches have adapted over time in the sector and the impact of COVID-19 on recruitment.

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

- Almost half of cyber sector businesses (47%) have tried to recruit someone in a cyber role since the beginning of 2019, most commonly using recruitment agents (48% of firms with vacancies), social networks such as LinkedIn (35%) and word-of-mouth recommendations (33%)
- Employers report that over a third (37%) of all the vacancies posted since the start of 2019 have been hard to fill. The most common reason given for this continues to be around candidates lacking technical skills or knowledge (48% of employers with hard-to-fill vacancies) but mentions of a lack of work experience have increased since 2020 (from 8% to 35%)
- The most common specialist skills shortage vacancies are in senior management roles, penetration testing and security architecture

6.1 Approaches to recruitment

Almost half of cyber sector businesses (47%) have tried to recruit someone in a cyber role since the beginning of 2019. The rest of the survey findings in this chapter focus on this 47 per cent of the sector (and later on those that have specifically had hard-to-fill vacancies).

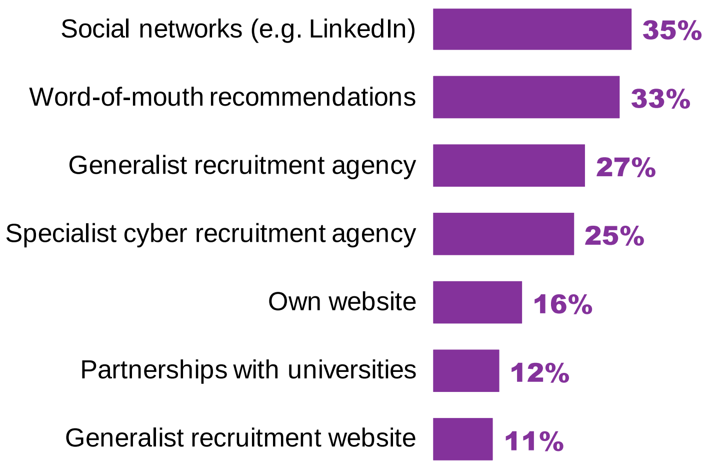
Most common recruitment methods

Figure 6.1 shows the most common recruitment methods used to find candidates for cyber roles, among the 47 per cent of businesses that have posted vacancies. While the cyber leads participating in the qualitative research highlighted various challenges and frustrations when using recruitment agents (detailed later in this chapter), this remains among the most common way of recruiting candidates. Around a quarter each use generalist recruitment agents (27%) or specialists (25%) which, when combined, equates to half of cyber sector employers with vacancies (48%).

The use of social networks (such as LinkedIn), and offline networking (e.g. with industry colleagues, or at events and conferences) is especially common, with each recruitment method being adopted by a third of the cyber sector employers with vacancies.

Broadly, these proportions are not significantly different from the 2020 survey. However, there has been a shift in the rankings of each response, which suggests that this year there may have been less use of recruitment agents and greater use of social networks. LinkedIn was frequently mentioned in the qualitative research. This might be expected, with COVID-19 potentially leading businesses, at least temporarily, to reduce external recruitment fees – although the qualitative research detailed later in this chapter paints a more mixed picture of the impact of COVID-19.

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



Base: 81 cyber sector businesses that have had vacancies in cyber roles since the start of 2019
Only specific categories mentioned by 10% or more shown.

As the chart shows, 12 per cent of those with vacancies have engaged in partnerships with universities to recruit new staff. By contrast, it is relatively rare to see partnerships with schools or colleges (5%) and for these employers to have specific graduate schemes (5%) – both these responses are not shown on the chart as they are under 10 per cent.

Current recruitment approaches are not especially diverse. 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 third (32%) have used 2 methods and around 1 in 6 (17%) have used 3 or more methods. These results may indicate a narrowing of the recruitment methods being used compared to last year (e.g. 37% used 3 or more methods in 2020), although the different timeframes for job vacancies covered in the 2020 and 2021 studies may also partly explain this change.

The dominance of personal networks

The qualitative research provides insights into why personal networks and word-of-mouth recommendations are so popular within the cyber sector.

Interviewees from the cyber sector commonly said that they would use personal networks for recruitment in the first instance, and would only fall back on recruitment agents if they could not find someone via their networks. There was a great deal of trust in word-of-mouth recommendations from others in the sector. There was a sense that people recruited in this way were a known entity, so it was a less risky form of recruitment. And other advantages were raised, such as not having to pay recruitment agents, and filter through a high volume of candidates.

Recruitment agents also made use of referrals and networking at technology or cyber security conferences and events to build their databases of job candidates.

"A lot of clients we get comes from mutual contacts, word of mouth – and that counts a lot in this industry."
Recruitment agent

The use of networks may have implications for diversity in the sector. One cyber sector interviewee remarked that employers in the sector tended to all go to the same university recruitment fairs, so saw a relatively narrow set of candidates. However, they felt that their business did not have the capacity to do anything more innovative or wide-reaching.

Personal networks were considered an especially important channel for senior roles. This be an additional factor driving the lack of diversity at senior levels within the sector.

Working with recruitment agents (both generalist and specialist recruiters)

The organisations we interviewed qualitatively tended to use recruitment agencies grudgingly. They often had strongly negative views of agents when it came to recruiting for cyber roles. We spoke to some that had developed good relationships with specific agents over a number of years, but they often considered these relationships to be the exception to the rule. Others used agents on a transactional, job-by-job basis. In these discussions, cyber employers did not make a distinction between the recruitment agents specialising in cyber security and more generalist recruitment agents.

Some interviewees felt that recruitment agents should be used as a last resort, when other methods did not work out (as noted in the previous section). The perceived advantage of using agents was that they could filter through candidates to find the right people for the role, but there were common criticisms about agency fees, being flooded with candidates, unsolicited contacts, and salary inflation.

"That is our least preferred option because we feel it incentivises poor behaviour and inflation of salaries."
Cyber sector business

Some recruitment agents themselves acknowledged the poor reputation of their industry in cyber recruitment. One interviewee noted that this was related to the traditional model of recruitment, which was based on posting adverts on job boards and maintaining a large database of candidates. In their view, successful cyber roles were typically too specialised to recruit in this way. They suggested that only 1 in 10 of their placements in the past year had been from replies to job boards.

Some agents said that they preferred to develop an ongoing dialogue with cyber employers and would ideally have wanted, in past experiences, to have more verbal conversations with hiring managers. In some cases, their interactions had mainly been with HR staff, who were regarded as poor at giving feedback and more reluctant to engage with specialist cyber recruitment agencies. There was also a sense that cyber employers sometimes unknowingly encouraged a more transactional approach, using several agencies to fill a single vacancy, and that this incentivised CV flooding, so an agent could fill the vacancy as quickly as possible.

Interaction with HR colleagues during recruitment

We also explored the role of HR colleagues in the qualitative research. As might be expected, smaller firms did not have an in-house HR function, so all aspects of recruitment were left to hiring managers. In larger firms with HR staff, these colleagues often helped with job descriptions and other elements of the recruitment process, such as arranging interviews and screening CVs for minimum requirements.

However, there were various examples of firms that had HR staff, but where these colleagues had very light-touch involvement in cyber recruitment. We heard only one example of HR staff offering advice around unbiased recruitment. In one case, an interviewee told us that their HR lead had complained about being brought in at the last minute on recruitment, and they typically got more involved in onboarding new joiners rather than recruiting staff. These findings suggest that HR staff could play an important role in increasing diversity in cyber roles through recruitment, but this would require more dialogue between HR colleagues and hiring managers.

6.2 What are employers looking for in recruitment?

Key recruitment criteria and filtering of candidates

Alongside technical knowledge and skills, employers across the qualitative interviews said they were looking for a willingness to learn, problem solving abilities, commitment and, for entry-level candidates, an interest in cyber security.

Employers used various techniques in job interviews to try to tease out technical knowledge, as well as the broader qualities like real-life problem solving. For example, one cyber sector interviewee said that if job applicants talked a lot about tools and methods, they would get asked how they might apply these to a legacy system. Other firms carried out situational tests or asked applicants what they would do in specific scenarios.

Some employers made use of especially innovative approaches. One cyber business opted to recruit people who had a degree in a non-cyber subject but who had done a year’s training on cyber security at a digital skills academy in their region. Another cyber firm used an online tool to filter entry-level roles. It set various challenges for candidates and allowed them to see how quickly they solved them.

“It is a gamified environment of cyber challenges that they have to complete to a certain level to qualify for the interview … It is designed to de-risk.”

Cyber sector business

Another important attribute for employers in selecting candidates was soft skills. Linked to this, recruitment agents mentioned cultural fit within the business as a specific factor. As noted in Chapter 3, this could have implications for diversity in recruitment.

"You need technical skills to get the interview but soft skills to get the job."

Recruitment agent

Qualification requirements

The organisations outside the cyber sector tended to use qualifications to set minimum standards for recruitment. The Certified Information Systems Security Professional (CISSP) accreditation, the Certified Information Security Manager (CISM) and qualifications related to ISO 27001 were all mentioned. They were seen as a way to find candidates with a basic level of understanding and competence, and to have the organisation keep on top of relevant skillsets.

Conversely, some recruitment agents described this as a lazy way to recruit. One agent noted that a hiring manager's role tends to be about mitigating risk and, therefore, taking risks with recruitment was antithetical to their mindset.

Unrealistic requirements in job postings

A major theme emerging from the qualitative interviews was around cyber employers putting potentially unrealistic or unachievable criteria in job specifications. The frequent reliance on recruiting with the same set of qualification criteria, especially outside the cyber sector, was linked to this. One recruitment agent said that, in their experience, at least 30 per cent of job postings were "unfillable".

> ***"Job specs are unrealistic in most situations. They include everything they can into them, including every possible qualification … It's like they're getting them from unicorn.com."***
> *Recruitment agent*

There was also a sense from recruitment agents that the hiring managers who wrote job descriptions did not understand the labour market very well, and might be trying to recruit for 2 or 3 jobs in one. Some recruitment agents had, for instance, come across unlikely combinations of skillsets, such as a job specification for a Chief Information Officer that required them to be able to undertake penetration testing. In addition, agents raised examples of employers not understanding the balance of technical and governance, regulation and compliance (GRC) skills that they truly needed and simply asking for people who were experts in both these areas.

These interviewees felt that there was a need to educate hiring managers on the types of candidates that inhabited the recruitment pool, the multitude of potential cyber career pathways and the kinds of qualifications that were relevant for different roles. While recruitment agents did not offer specific solutions, this finding links to our study recommendation (see Chapter 8) to develop example job descriptions and suggested minimum qualifications for typical cyber roles.

6.3 Hard-to-fill vacancies and skills shortages

Among the 47 per cent of cyber sector firms that have had any cyber security vacancies since the start of 2019, almost 6 in 10 (57%) had at least one vacancy that they considered to be hard to fill. From another perspective, this equates to over a third (37%) of all the vacancies posted since the start of 2019 being hard-to-fill vacancies. This suggests that the size of the cyber security skills shortage has not changed significantly from 2020, when this was 35 per cent.

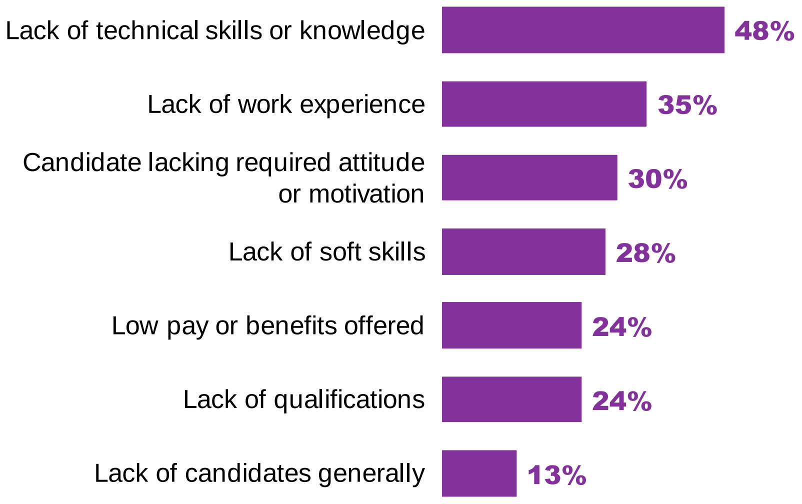
Reasons behind hard-to-fill vacancies

As Figure 6.2 shows, among the cyber sector firms that have had hard-to-fill vacancies, the single most common reason given for this (without prompting) is that applicants have lacked technical skills and knowledge. This highlights that relevant technical skills are the single most important element that employers are looking for when recruiting for cyber roles – consistent with the 2020 findings.

Nevertheless, it is worth noting the other common issues that arise. These include applicants lacking work experience, lacking the right attitudes or motivation, and lacking soft skills. Mentions of a lack of work experience have increased since 2020 (from 8% to 35%).

This year, none of the cyber sector firms surveyed mentioned their location as a reason behind hard-to-fill vacancies, compared to 10 per cent in 2020. This indicates that this has become a lesser issue than before. One impact of COVID-19 and the trend towards remote working has potentially been to enable job applicants to apply for jobs further afield – this chimes with the findings from the qualitative research covered in Section 6.5.

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



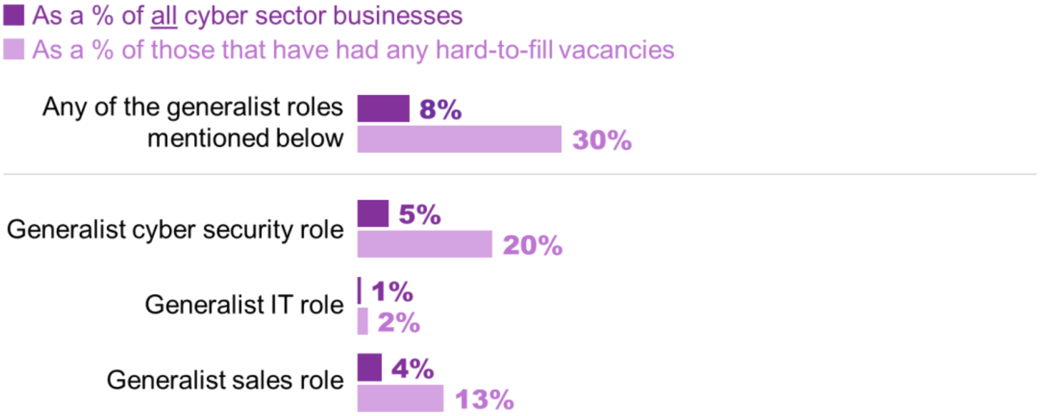
Base: 46 cyber sector businesses that have had hard-to-fill vacancies in cyber roles since the start of 2019
Only specific categories mentioned by 10% or more shown.

Specific roles most affected by skills shortages

The survey findings suggest that there is a mix of skills shortages across both generalist and specialist cyber roles, with a slant towards specialist roles. In this context, we mean generalist roles where someone might be expected to understand and discuss a wide range of cyber security areas, but not necessarily in depth.

Among the cyber sector businesses that have had hard-to-fill vacancies, just under 1 in 3 say they have had such vacancies in generalist roles (Figure 6.3). This amounts to around 1 in 10 cyber sector firms across the overall sector population. It includes positions that are formally labelled as cyber roles, 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: 171 cyber sector businesses; 46 that have had hard-to-fill vacancies in cyber roles since the start of 2019

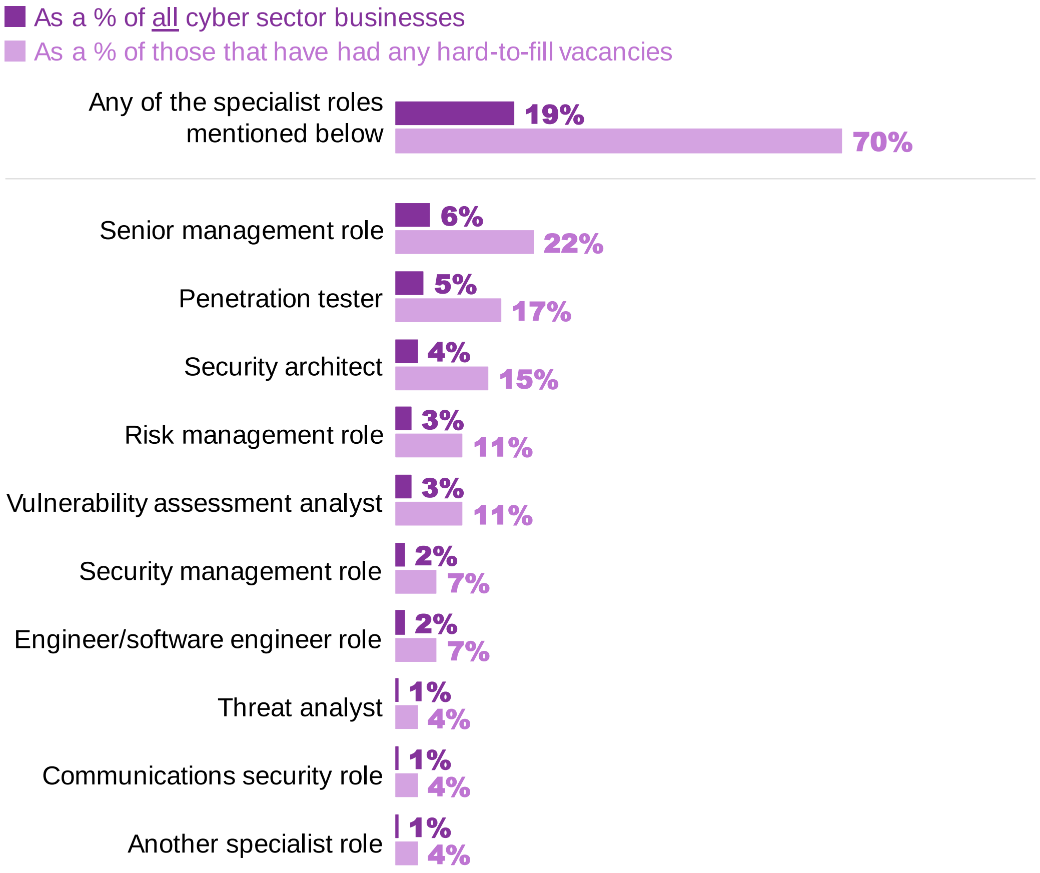
Among those that have had hard-to-fill vacancies, 7 in 10 have had such vacancies in specialist roles. This equates to a fifth of all cyber sector firms.

In Figure 6.4, we show how these hard-to-fill vacancies map to the Chartered Institute of Information Security (CIISec, formerly IISP) Roles Framework.[7] This framework covers 10 specialist cyber roles. The most common skills shortages are in senior management roles, penetration testing and security architecture. It is worth remembering that penetration testing and security architecture also come towards the top of the list of advanced skills gaps in the wider economy (Figure 4.5 in Chapter 4), while assurance, audits, compliance and testing are high on the list of skills in demand in cyber sector firms (Figure 4.6). In other words, it appears that employers are trying both to develop and improve these skills among existing staff and to recruit others to perform these roles.

The mentions of senior management roles have increased since 2020 (from 8%, to 22% now).

[7] In the survey, respondents are given a fuller description of each role, adapted from the descriptions in the Framework, if they 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: 171 cyber sector businesses; 46 that have had hard-to-fill vacancies in cyber roles since the start of 2019

In the qualitative research, interviewees raised the following roles, in addition to those mentioned in Figure 6.4, as being hard to fill:

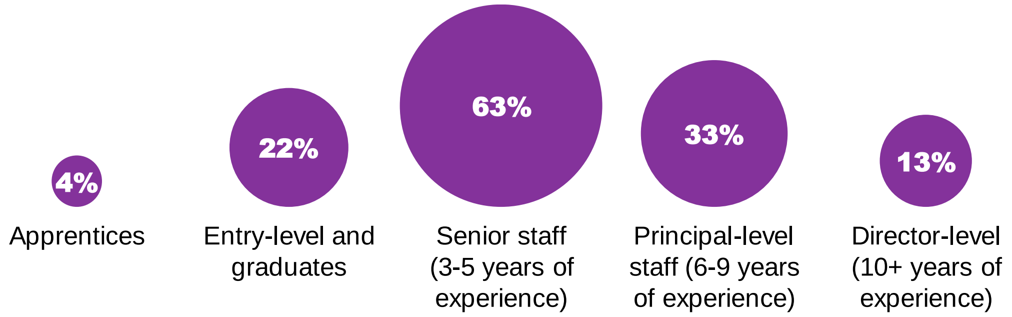
- Awareness and training roles
- Cyber security research roles, as these require especially in-depth technical knowledge which relatively few people in the market possess
- Roles related to cloud security (e.g. Cloud Security Architect was mentioned)
- DevSecOps roles, as an emerging area of cyber security
- Salespeople with a sufficient technical understanding of cyber security

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). This continues to match the findings from the job vacancies analysis (Chapter 7) showing the levels that vacancies are set at.

While these findings do not show any statistically significant changes from the 2020 survey, there has been a shift upwards in the figures for staff with 6 or more years of experience, and this ties in with the increased difficulties in recruiting senior management roles reported in the previous section.

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: 46 cyber sector businesses that have had hard-to-fill vacancies in cyber roles since the start of 2019

The findings in Figure 6.5 can be contrasted against our job vacancies analysis covered in Chapter 7 (specifically, Figure 7.8). This shows that, while principal and director level roles are, collectively, more likely to be hard-to-fill, there are relatively few firms across the economy posting jobs in these brackets, and far more posting core and cyber-enabled jobs in the entry-level bracket. Both sets of data continue to show that the skills *demand* and skills *gaps* are greatest for staff with 3 to 5 years of experience.

6.4 Implications of skills shortages in cyber teams

The qualitative research explored the impacts of cyber security skills shortages, both within the cyber sector and the wider economy.

Outside the cyber sector, cyber leads often found themselves working long hours, at the risk of burnout. In some instances, this reflected that senior managers in the organisation had underestimated the scale of tasks in cyber security (as noted in Chapter 4). Sometimes it was due to a lack of personnel to share workloads. For example, one interviewee reported working over 90 hours a week at one point, covering the entire cyber security framework themselves. Interviewees feared that these high workloads would lead to them missing risks.

Strategies to deal with these shortages include using contractors or temporary staff, or pulling in resources from other departments. One large cyber firm had also dealt with skills shortages in the UK by setting up resource hubs in Europe.

One cyber sector interviewee thought a common response to skills gaps was for organisations to bring in new processes and bureaucracy, for instance having more risk registers, rather than investing in extra personnel.

Within the cyber sector, some firms also noted, in line with the survey data (covered in Section 4.3), that a lack of cyber skills was a constraint on their growth.

"We cannot service market demand, so we cannot grow as quickly as we might."

Cyber sector business

6.5 The impact of COVID-19 on recruitment

In the qualitative research, across both the recruitment agent and cyber employer interviews, COVID-19 was expected to have the following impacts on recruitment, which might serve to reduce the issue of hard-to-fill vacancies for a time:

- There would be a bigger talent pool available, due to job losses in sectors negatively impacted by COVID-19. Aviation was raised as an example. This would result in more people with cyber security skills looking for work, and more people looking to transition into cyber security roles for the first time. One recruitment agent said, for instance, that they used to have 1 to 2 candidates approaching them every month, but now they had 10 to 20 a week

- Recruitment would become more geographically diverse, because more organisations would have adapted to remote working. We heard, for example, a case where a cyber firm based in the North of England had just hired someone located in Northern Ireland

> ***"The rhetoric I've used with my hiring managers is find us the best person for the best price anywhere in the UK. From the highlands to Cornwall, which would not historically be our employment target areas."***
> *Cyber sector business*

At the same time, some of these impacts might be dampened by other trends. Some interviewees said that, in the current climate, it is natural that fewer people will take the risk of leaving their jobs, so staff turnover would fall. Some of the organisations we spoke to had also implemented recruitment freezes. One cyber lead said, for instance, that their plans to recruit a junior network support staff member with knowledge in network security had been put on hold indefinitely as a result of COVID-19.

7 Cyber security job vacancies

This chapter sets out an analysis of cyber security job vacancies, based on our analysis of the secondary job data on 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 primarily covers vacancies posted from January 2020 to the end of December 2020, i.e. 12 months of data. Last year's labour market report was the first to incorporate this strand of the research, so covered a longer period of job vacancies from September 2016 to August 2019 (3 years of data) to form a robust baseline. We therefore make comparisons, where possible, between the 12 most recent months and this baseline. In addition, the first two charts in this section show the monthly change in job postings over a longer time period, to cover trends before and since the start of the COVID-19 pandemic.

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 more accurately show these subtle variations.

Key findings

- The number of job postings fell by around one-third following the first COVID-19 lockdown in March 2020. But it has returned to, and remained at, pre-COVID levels since Autumn 2020
- In the latest 12 months, compared to the previous 3 years, there has been a slight fall in the proportion of job vacancies that are in London, against some small increases in the North West, Northern Ireland, and the East Midlands
- There is evidence that towns and cities such as Reading, Bristol, Leeds, Belfast, and Bath are expanding the proportional size of their cyber security sectors within their local labour markets
- Compared to the previous 3 years, employers are placing greater emphasis on hiring those with at least 3 to 5 years of experience
- Remuneration has remained relatively constant within the cyber security labour market compared to the previous 3 years, with the average advertised salary for a core cyber security role being £59,200. This may mask regional variation, with a stronger drop seen in Wales

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 report, 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 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 2, 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

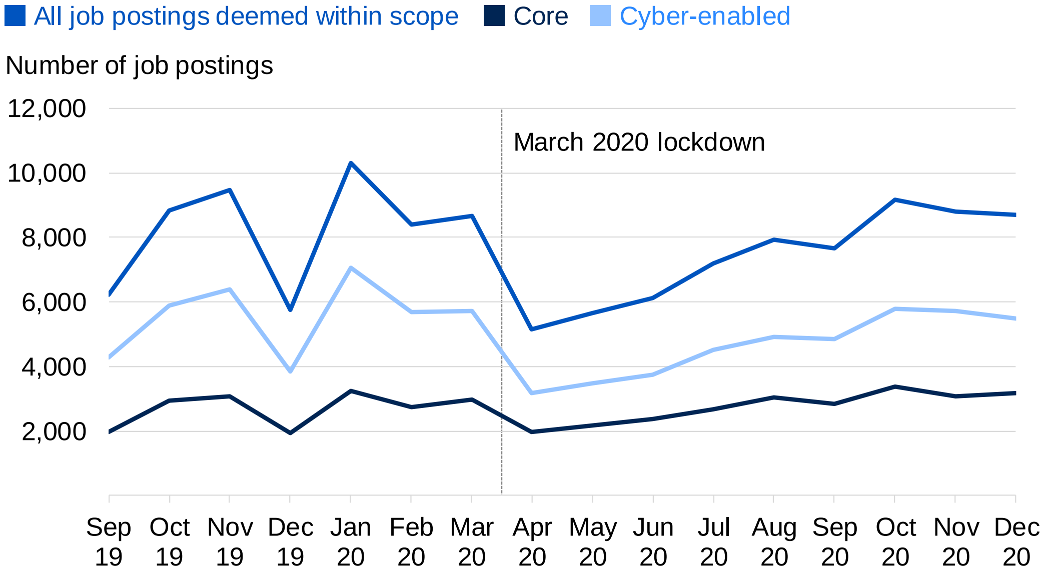
Figure 7.1 shows the monthly trend for a period of 16 months from September 2019. This date starts off where the data from the previous report (covering job postings up to August 2019) finished. The previous 3-year baseline found that there were approximately 11,000 cyber security-related job postings each month, of which c.3,000 per month were for core cyber roles.

For the newest data, between September 2019 and December 2020, we have identified 124,016 cyber security-related job postings. Of these:

- 43,517 are core cyber security roles (an average of c.2,700 per month)
- 80,499 are cyber-enabled roles (an average of c.5,000 per month)

The newest data highlights how the number of job postings fell substantially in late March and early April following the first COVID-19 lockdown (which started on 26 March), but broadly recovered to pre-lockdown levels in Autumn 2020.

Figure 7.1: Monthly number of core and cyber-enabled online job postings from September 2019 to December 2020



Source: Burning Glass Technologies
Base: 124,016 online job postings from September 2019 to December 2020 (of which 93,747 were in 2020); 43,517 core; 80,499 cyber-enabled

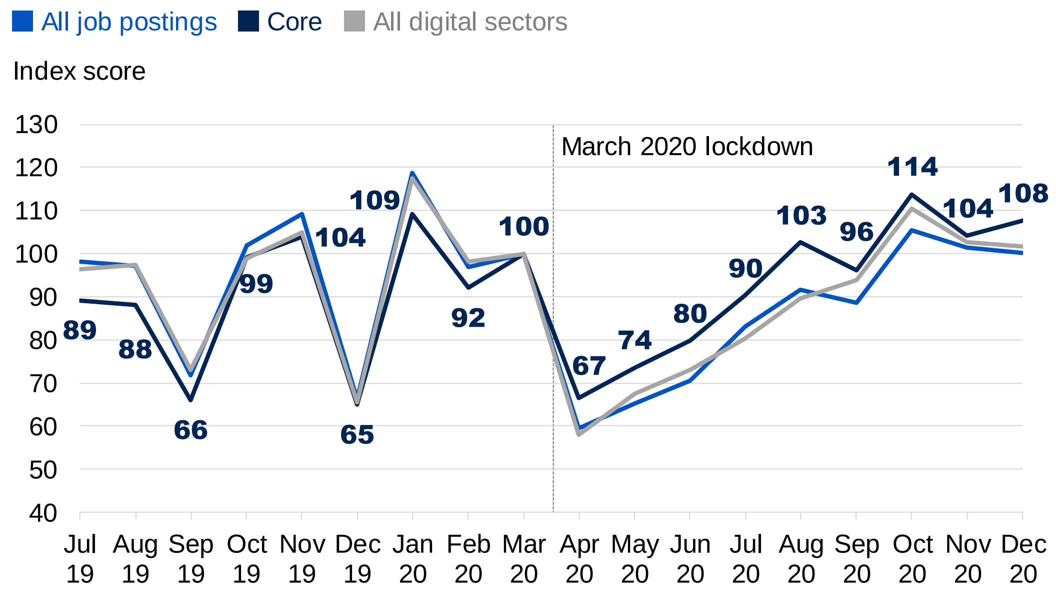
Figure 7.2 specifically demonstrates how the volume of cyber security job postings has changed since March 2020. The job postings for all other months are indexed to this month, which has a score of 100. In other words, the score for each subsequent month shows the per cent change in vacancies compared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

There was a 33 per cent drop in the number of core cyber job vacancies between March and April 2020. However, the labour market appears to have recovered lost ground by August 2020. Indeed, in October 2020, there were 3,369 core cyber roles posted, which is 14 per cent above the March 2020 level, indicating the speed and extent of the recovery.

As the chart shows, this recovery has largely followed the trend for the wider digital sector, but core cyber roles have broadly had less of a drop-off and a stronger recovery than digital job roles overall.[8]

[8] This reflects the DCMS definition of the digital sector, covered in the DCMS Sectors Economic Estimates Methodology.

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



Source: Burning Glass Technologies
Base: 140,951 online job postings from July 2019 to December 2020; 48,763 core; 1,015,633 across all digital sectors

Benchmarking against other cyber security employment estimates

Beyond this research project, there have been other attempts within the last 12 months to understand the size and scale of the cyber security workforce in the UK, and to understand gaps in supply:

- DCMS's Cyber Security Sectoral Analysis 2021 estimates 46,683 full-time employees working in cyber roles in the UK cyber sector, across the 1,483 cyber security companies that make up this sector. However, this excludes individuals working in cyber roles outside of these companies

- Also, recently, the 2020 (ISC)^2 Cybersecurity Workforce Study report has estimated that there are c.366,000 people in the UK cyber security workforce

In our view, the (ISC)^2 estimate is too high. Ipsos MORI and Perspective Economics modelling, carried out as part of the separate DCMS research on the cyber security recruitment pool, suggests the UK cyber security workforce (across the entire economy) is likely to be in the range of c.112,000 to c.174,000 individuals. This is the most comprehensive research on the size of the recruitment pool date and covers a wide range of sources.

7.3 Geographic differences

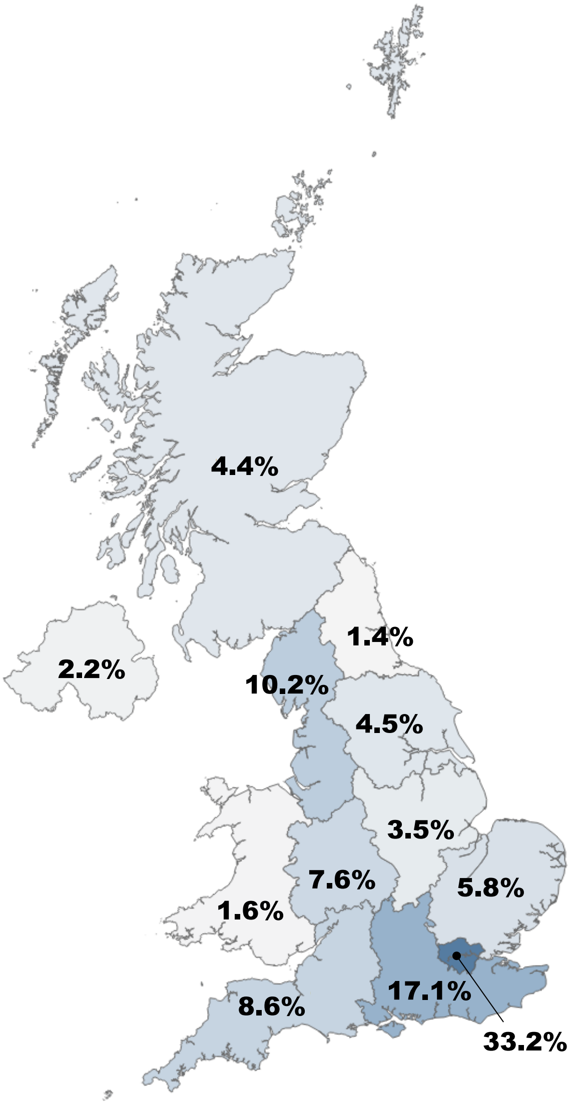
The rest of this chapter focuses on the job postings from January to December 2020, i.e. for a 12-month period.

Figure 7.3 shows the proportion of job postings for core cyber roles from each UK region (where the region is known) for 2020. 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.

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

Ranking

1. Greater London (33.2%)
2. South East (17.1%)
3. North West (10.2%)
4. South West (8.6%)
5. West Midlands (7.6%)
6. East of England (5.8%)
7. Yorkshire and the Humber (4.5%)
8. Scotland (4.4%)
9. East Midlands (3.5%)
10. Northern Ireland (2.2%)
11. Wales (1.6%)
12. North East (1.4%)



Source: Burning Glass Technologies
Base: 29,344 core cyber job postings from January to December 2020 where region was listed (out of a total 33,622)
Map created using OpenStreetMap data in Mapbox

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 within London, in parts of the North West, parts of the West Midlands and along the M4 corridor.

We have, therefore, carried out more granular geographic analysis using the Travel to Work Areas (TTWAs) in the UK.[9] 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.

[9] 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.

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.

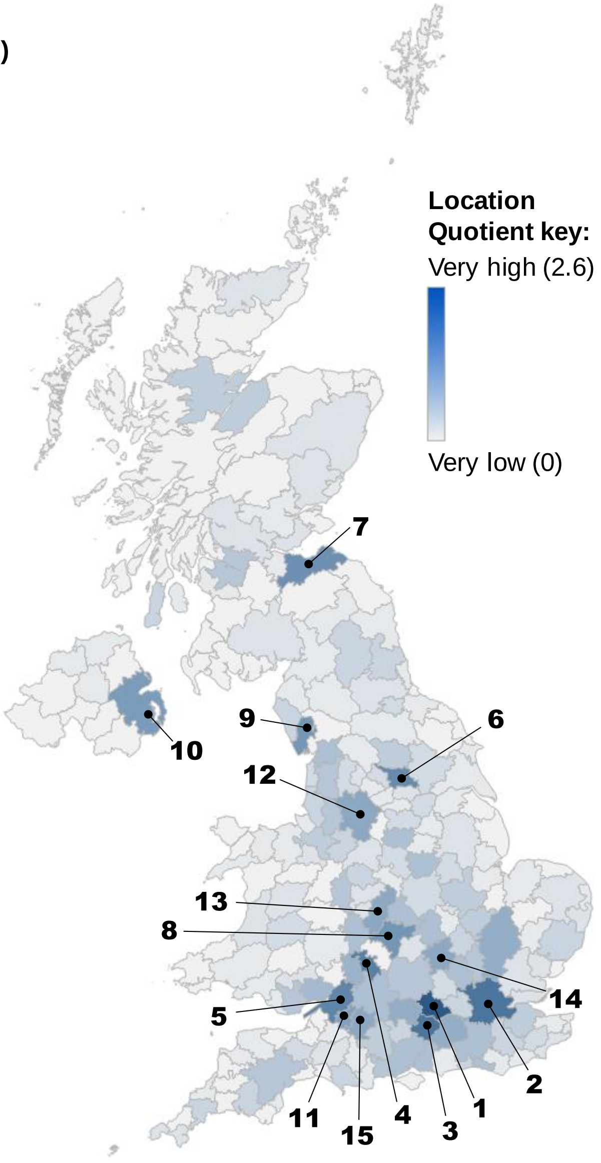
Figure 7.4: Number of core cyber job postings and Location Quotients in the top 15 UK Travel to Work Areas

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

i. London (9,404)
ii. Manchester (1,393)
iii. Birmingham (915)
iv. Bristol (787)
v. Reading (765)
vi. Leeds (695)
vii. Belfast (603)
viii. Edinburgh (569)
ix. Cambridge (406)
x. Glasgow (381)
xi. Guildford and Aldershot (347)
xii. Slough and Heathrow (331)
xiii. Luton (287)
xiv. Nottingham (282)
xv. Basingstoke (280)

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

1. Reading (2.6)
2. London (2.0)
3. Basingstoke (2.0)
4. Cheltenham (1.8)
5. Bristol (1.7)
6. Leeds (1.6)
7. Edinburgh (1.5)
8. Leamington Spa (1.4)
9. Barrow-in-Furness (1.4)
10. Belfast (1.3)
11. Bath (1.2)
12. Manchester (1.1)
13. Birmingham (1.1)
14. Milton Keynes (1.1)
15. Trowbridge (1.1)



Source: Burning Glass Technologies
Base: 24,759 core cyber job postings from January to December 2020 where TTWA was listed (out of a total 33,622)
Map created using OpenStreetMap data in Mapbox
The Isle of Man and the Channel Islands are not TTWAs so are not included.

Looking across both these maps 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 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 like Wales and the East Midlands, there are a small number of very large firms that dominate the local cyber security labour market –

DCMS's Cyber Security Sectoral Analysis 2021 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 underrepresent these types of employers.

Changes over time

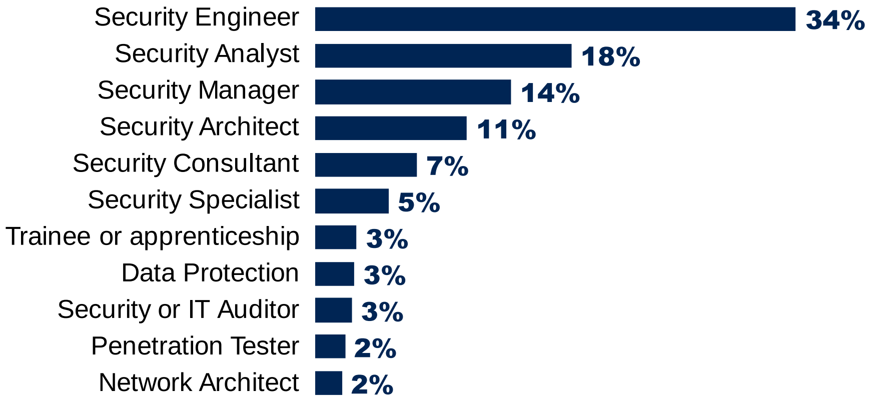
This geographic spread in Figure 7.3 is largely consistent with last year's analysis, which covered job postings from September 2016 to the end of August 2019. However, there has been a slight reduction in the proportion of job vacancies in London (down from 35.5% to 33.2%) and the West Midlands (down from 9.5% to 7.6%). On the flipside, there has been a noticeable increase in the North West (7.1% to 10.2%), the East Midlands (2.6% to 3.5%) and Northern Ireland (1.5% to 2.2%).

These regional shifts may be indicative of the large trend towards home working, as a result of the COVID-19 pandemic. As the qualitative research indicates (see Section 6.5), recruiters and employers expected there to be applications from a more geographically diverse set of candidates due to this trend.

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.[10] Security engineering roles are 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: 15,050 core cyber job postings featuring one of the top 200 job titles (across all 33,662 core cyber job postings) from January to December 2020

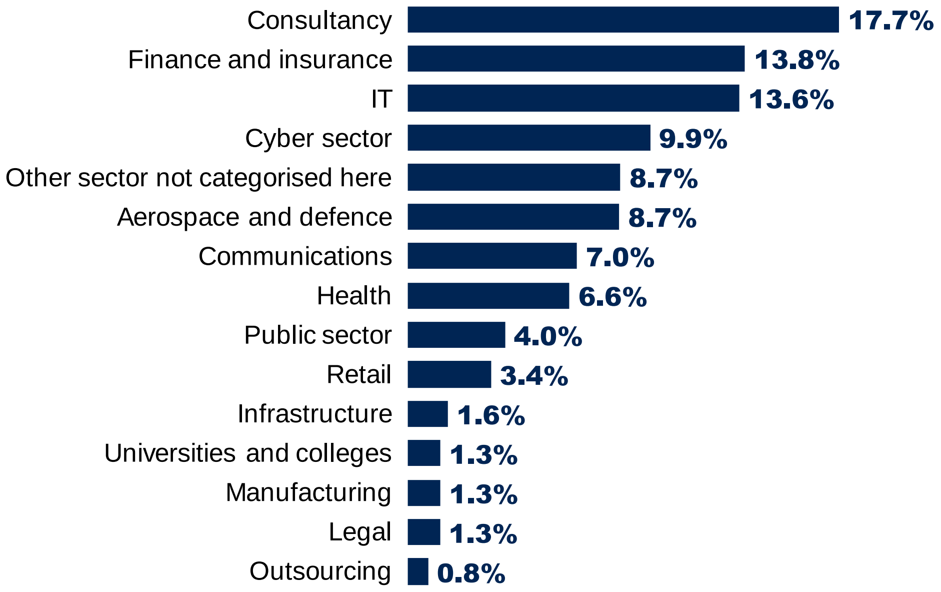
This is not directly comparable with the equivalent chart from last year's report, which focused on the top 20 job titles without combining similar variations. However, broadly speaking, both this year's and last year's data shows that the top five roles sought have remained consistent across the last four years: security engineers, analysts, managers, architects and consultants. It is worth noting that these are very broad titles that do not necessarily convey the core functions of the role, potentially reflecting the current lack of a standardised cyber security careers framework.

[10] 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, covering 15,050 of the total 33,662 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 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 5,539 job postings for the latest 12 months (around 16% of all the core cyber job posts identified) have a known employer name[11] and we have categorised these by their sector (Figure 7.6).[12]

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: 5,539 core cyber job postings from January to December 2020 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. It suggests that the sectors most in demand of cyber talent are the finance and insurance, information and communications, and professional services sectors.

Matching the employers against the DCMS list of UK providers of cyber security products and services shows that 9.9 per cent of these job postings are from cyber security firms. However, looking at the specific company names suggests that some of the UK's leading cyber security firms have a relatively low volume of job postings within the dataset. This suggests that many top cyber firms are, in fact, recruiting through agencies, headhunters or other platforms – although to a lesser extent than before.

Changes over time

Compared to last year's report, there has been a softening in demand from the finance and insurance sector (down from 22.5% to 13.8%), retail (down from 7.8% to 3.4%) and the public sector (7.7% to 4.0%). There has been an increase from consultancy businesses (from 15.5% to 17.7%) and cyber

[11] 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.
[12] These are not SIC 2007 sectors, but more comprehensible sector groupings sometimes determined by the product or service offer.

sector employers (from 4.9% to 9.9%). This may suggest that, compared to previous years, more cyber firms have been recruiting directly rather than through agencies across 2020.

7.6 The skills, qualifications and experience being demanded

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

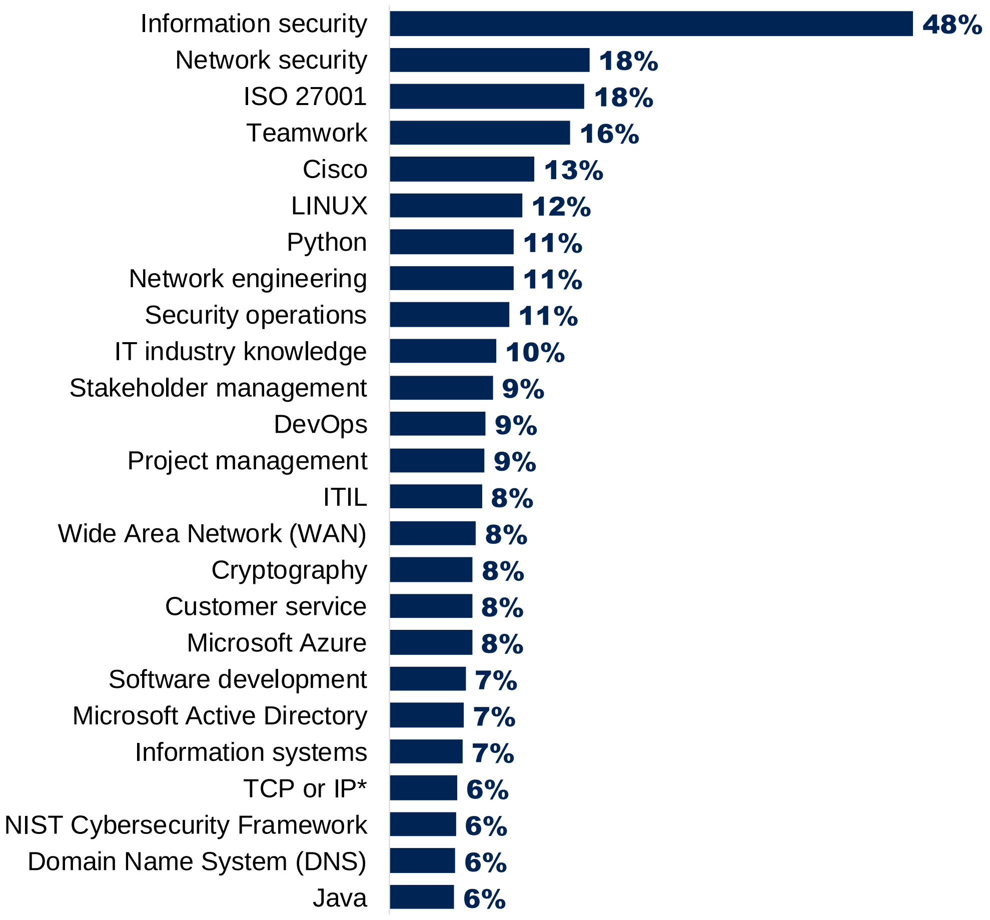
Skills in demand

Looking at core cyber roles, the top 3 skills requirements mentioned in job descriptions remain information security skills, network security skills and skills around ISO 27001 (the international information security standard). The full list is in Figure 7.7.

The next most commonly demanded technical skills areas can be summed up as follows, and are similar to those covered in last year's report:

- Network engineering (e.g. Cisco and Juniper)
- Risk management and technical controls (e.g. ISO 27001 and ITIL)
- Operating systems and virtualisation (e.g. Linux and VMWare)
- Cryptography
- Programming (e.g. Python, Java and SQL)

Figure 7.7: Top skills requested for core cyber job roles



Source: Burning Glass Technologies
Base: 27,260 core cyber job postings from January to December 2020 that request at least one specific skill
*TCP or IP stands for Transmission Control Protocol (TCP) or Internet Protocol (IP).

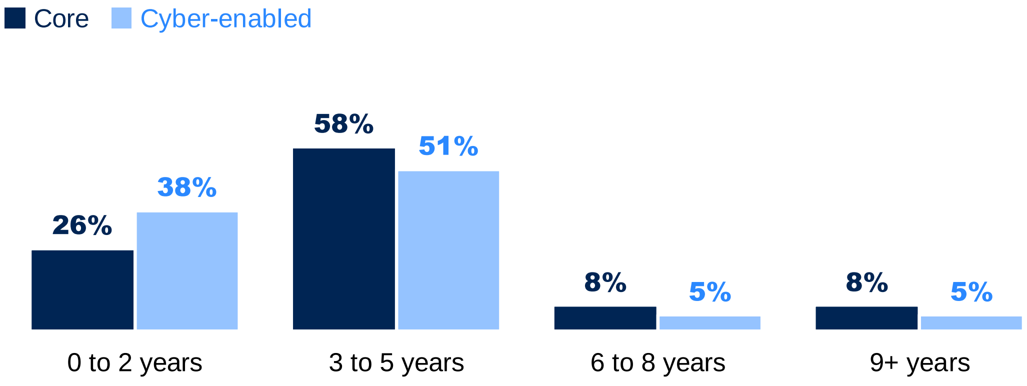
Both the top 2 terms here appeared less in job descriptions in the latest 12 months than in the earlier 3-year period covered in last year's report. Information security is down from 61 per cent to 48 per cent. Network security was 22 per cent last year (now 18%). This suggests that these core cyber job postings have, on the whole, become more specific over time with their requested skillsets.

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 (58%), followed by entry level applicants (26%).

In cyber-enabled roles, there is greater demand for those in entry level positions (38%, vs. 26% of core cyber job postings). This highlights the ongoing reluctance of employers to take on dedicated (i.e. core) cyber staff at the entry level.

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): 5,504 core cyber job postings from January to December 2020; 14,459 cyber-enabled job postings over this period

The demand for core cyber job candidates with 3 to 5 years of experience has increased (from 52% in last year's study to 58% this year). This could indicate that employers are further entrenching their positions of wanting job-ready candidates. Alternatively, it could reflect findings from the qualitative research with recruitment agents and employers, that the COVID-19 pandemic has increased the talent pool (see Section 6.5), allowing employers to more easily demand experienced candidates.

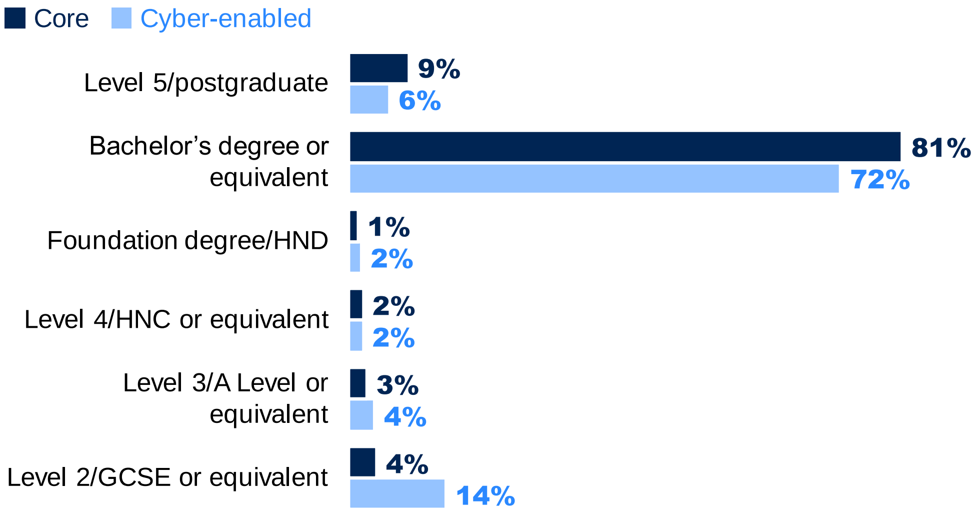
Education requirements

As Figure 7.9 shows, employers continue to place a strong emphasis on applicants having bachelor's degrees or higher qualifications.

In fact, compared to last year's report, the proportion requesting a postgraduate qualification has slightly increased (from 6% to 9%). This may be a sign that employers are placing a greater emphasis on a higher education than before. Alternatively, as noted in the previous section, it could be that employers have more flexibility to make these demands, as the talent pool has increased due to COVID-19.

There are differences between core and cyber-enabled job roles. Employers looking to fill cyber-enabled job roles are more than twice as likely to accept A Levels or GCSEs as a minimum (18% vs. 7%). This reflects the fact that cyber-enabled roles are more likely to include support positions and entry-level positions. They therefore may not be as dependent on technical or educational backgrounds.

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): 6,313 core cyber job postings from January to December 2020; 14,834 cyber-enabled job postings over this period

Demand for certifications

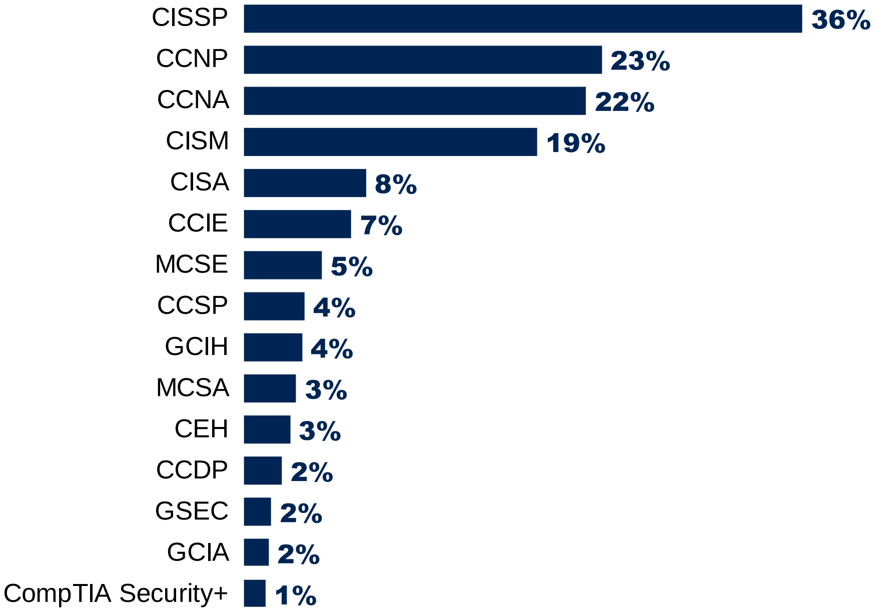
The most commonly requested certification remains the Certified Information Systems Security Professional (CISSP), which is included within 36 per cent of the job postings that ask for a specific certification. In previous years, our research has highlighted that:

- 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

Cisco Certified Network certifications continue to be in high demand, with 23 per cent requesting Cisco Certified Network Professionals (CCNP), 22 per cent requesting Cisco Certified Network Associates (CCNA), and 7 per cent requesting Cisco Certified Internetwork Experts (CCIE).

The top-ranking certifications are shown in Figure 7.10. This list and the proportions show a great deal of consistency with last year's analysis (covering the previous 3-year period). For example, CISSP was 37 per cent in last year's report, while CCNP was 27 per cent and CCNA was 22 per cent.

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



Source: Burning Glass Technologies
Base: 6,681 core cyber job postings from January to December 2020 that request specific certifications

This analysis does not specify whether employers are requesting specific versions of the certifications shown in Figure 7.10. The version was often, as per last year's analysis, not specified in the job description – a further challenge for individuals navigating the training market.

7.7 Salaries

Across the latest 12 months, the mean advertised salary was £59,200 for a core cyber job posting (with a median value of £53,000). The mean advertised salary was £47,900 for all cyber job postings (with a median of £40,700).

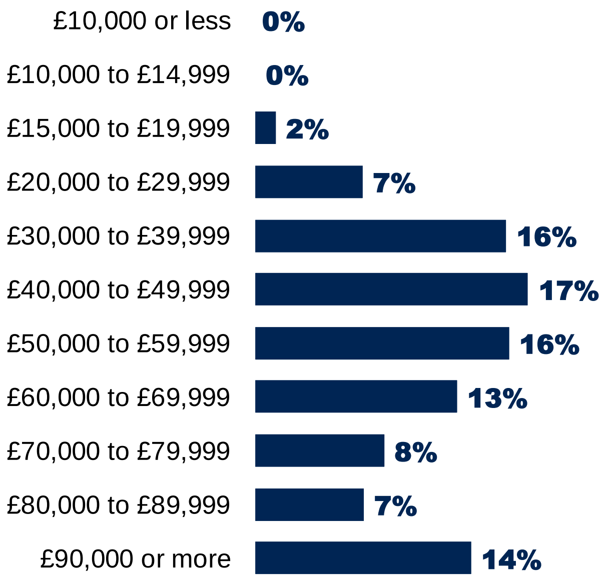
As a comparison, for all employee jobs within SIC code 62, which is the computer programming, consultancy and related activities industry code, the mean annual pay in 2020 was £50,130 (with a median of £41,078).[13] Using this value as a proxy for IT jobs in the UK suggests there is still a wage premium of approximately 29 per cent for core cyber security jobs compared both to IT jobs as a whole, and jobs with a partial cyber security requirement (when comparing median salaries).[14]

All our salary analysis only relates to advertised job postings. It is important to remember that many cyber security job vacancies can have a flexible salary structure depending on candidate skills and experience.

[13] This is sourced from the Office for National Statistics (ONS, 2020) Annual Survey of Hours and Earnings.

[14] 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).

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



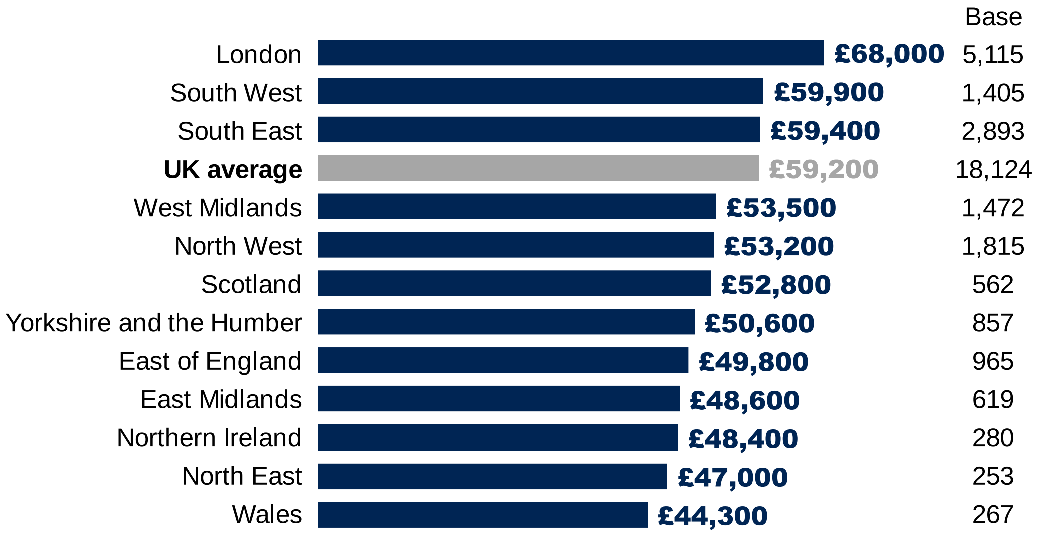
Source: Burning Glass Technologies
Bases 18,124 core cyber job postings from January to December 2020 that mention salaries or salary bands

Geographic variation in salaries

London continues to have the highest mean advertised salary for core cyber roles. This is expected, given the prevalence of the finance sector as well as higher typical costs of living in the capital.

At the other end of the market, Wales has considerably lower average advertised salaries for core cyber security roles (a mean of £44,300, vs. the national average of £59,200).

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 (16,503 of the 18,124 job postings with salary data can be mapped to a specific UK region – the other 9% are based in the UK but may include national or remote locations)

Changes over time

In last year's analysis, the mean advertised salary for a core cyber job role was £59,600 (with a median value of £55,000). The mean advertised salary for all cyber jobs within the dataset (i.e. including cyber-enabled jobs) was £46,900 (with a median of £40,000). As such, the advertised salaries across cyber roles have, on the whole, neither notably increased nor decreased in 2020 versus the previous 3 years.

This overall picture masks regional changes. Table 7.1 shows that most regions have reported a modest decline, whereas Wales shows a more substantial decline of 13.1 per cent. By contrast, the mean advertised salary in Northern Ireland has increased by 11.8 per cent, with other less substantial increases seen in the South West, West Midlands and the South East. However, any annual change figures should be treated with caution and used in conjunction with other evidence (e.g. from recruiter surveys) – it may, for example, be especially skewed by any changes in advertised salary practices by larger employers.

Table 7.1: Change over time in mean salary offers for core cyber job postings by region (where the salary or salary range is advertised)[15]

Region	Sep 2016 to Aug 2019	Jan to Dec 2020	Change since last year's study
Northern Ireland	£43,300	£48,400	+£5,100 (+11.8%)
South West	£56,100	£59,900	+£3,800 (+6.8%)
West Midlands	£51,000	£53,500	+£2,500 (+4.9%)
South East	£58,500	£59,400	+£900 (+1.5%)
UK average	**£59,600**	**£59,200**	**-£400 (-0.7%)**
Yorkshire and the Humber	£51,000	£50,600	-£400 (-0.8%)
London	£68,900	£68,000	-£900 (-1.3%)
North West	£54,100	£53,200	-£900 (-1.7%)
East of England	£51,600	£49,800	-£1,800 (-3.5%)
Scotland	£54,900	£52,800	-£2,100 (-3.8%)
North East	£49,000	£47,000	-£2,000 (-4.1%)
East Midlands	£51,200	£48,600	-£2,600 (-5.1%)
Wales	£51,000	£44,300	-£6,700 (-13.1%)

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

8 Staff turnover in the cyber sector

This chapter covers new content from this year's survey measuring staff turnover within the cyber sector and the reasons why staff have left their posts (where employers are aware of the reason).

Key findings

- A total of 6 per cent of the cyber workforce (within the cyber sector) are estimated to have left their posts since the start of 2019, with 4 per cent leaving of their own volition
- The most common reason employers give for staff leaving of their own volition is because of a lack of pay or benefits offered (43% of the employers who have had staff leave)

8.1 An estimate of cyber workforce staff turnover

We estimate that 6 per cent of the cyber workforce (within the cyber sector) left their posts in the 18 months since January 2019. 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).

A total of 4% left of their own volition, with the remaining 2% being relatively equally distributed between retirement, redundancy and dismissal (all adding to 1% or under 1%).

8.2 Why employees leave their roles

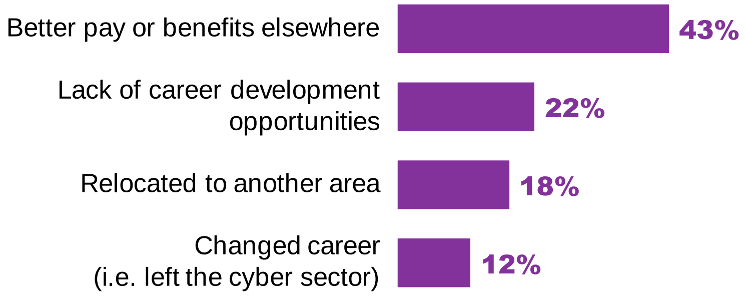
The 6 per cent estimate breaks down as follows:

- 4 per cent left of their own volition
- 1 per cent retired
- 1 per cent were dismissed

In the 4 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 7.1, covers employers' *perceptions* of why these employees left their posts, which may be different from employees' own views.

The most common reason offered by employers is that staff left to get better pay or benefits elsewhere. While 18 per cent mention that staff left because they moved to another part of the country, only 6 per cent say specifically that they are based in a remote location with poor transport links – this latter response is not shown on the chart.

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: 49 cyber sector businesses that have had employees leave since the start of 2019
Only specific categories mentioned by 10% or more shown.

The qualitative research with recruitment agents also provided insights as to why people leave cyber roles. The feedback highlights that, while salary remains one of the top considerations for job applicants, the working culture can also be a driving factor in people leaving. This includes lack of career progression and training, as per Figure 8.1. It also includes, outside the cyber sector, an organisation's senior management not valuing cyber security and sustaining a poor cyber security culture. We also heard difficult working environments (e.g. a poor line manager) being a reason. In the view of one agent, employers were felt to overestimate the importance of salary relative to working culture.

There was a distinction drawn between people actively looking for new jobs and passive candidates, who are not actively looking. The latter were felt to be more likely to leave if the role offered meant that they could have more impact, for instance by being involved with a new programme of work.

We also heard examples from recruitment agents where female employees had specifically left the industry because of company culture and difficulties in progressing further in their careers. This may be one reason behind a lack of diversity in senior levels.

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.

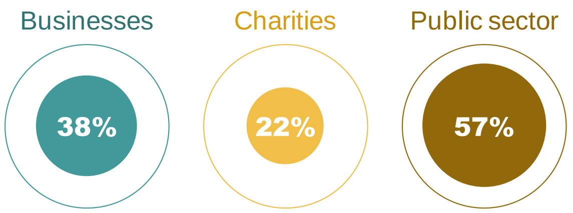
Key findings

- Around 4 in 10 businesses (38%) outsource any aspects of cyber security, compared to around 6 in 10 public sector organisations (57%)
- Setting up firewalls, incident response and detecting malware are the 3 most commonly outsourced cyber security functions (by around 8 in 10 of the businesses that outsource). Among the 38 per cent of firms that outsource cyber security, 56 per cent specifically outsource functions that require more advanced technical skills, such as interpreting malicious code
- External Security Operations Centres (SOCs) tend to be more common in public sector organisations (56% of those outsourcing) than private sector ones (39% of those outsourcing)

9.1 The prevalence of outsourcing

Around 4 in 10 businesses outsource any aspects of cyber security (Figure 8.1). This proportion is lower among charities and higher among public sector organisations. The pattern of results is consistent with the 2020 findings and suggests that outsourcing remains more common than in 2018 (when 30% of private sector businesses said that they outsourced cyber security).

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



Bases: 965 businesses; 220 charities; 76 public sector organisations

Outsourcing is more common among non-micro businesses. In fact, around half or more of small (54%), medium (58%) and large businesses (51%) outsource at least part of their cyber security. This remains on a par with last year’s findings.

Outsourcing is more prevalent within sectors like finance and insurance (66%, vs. 38% on average) which was also the case in the 2020 survey. Information and communications businesses are less likely than others to outsource any aspects (28%, vs. 38% overall). It is worth remembering that the information and communications sector grouping includes IT consultancy, maintenance and other IT services, so it might be expected that more of these kinds of firms would keep their own cyber security in-house.

9.2 What aspects of cyber security do organisations outsource?

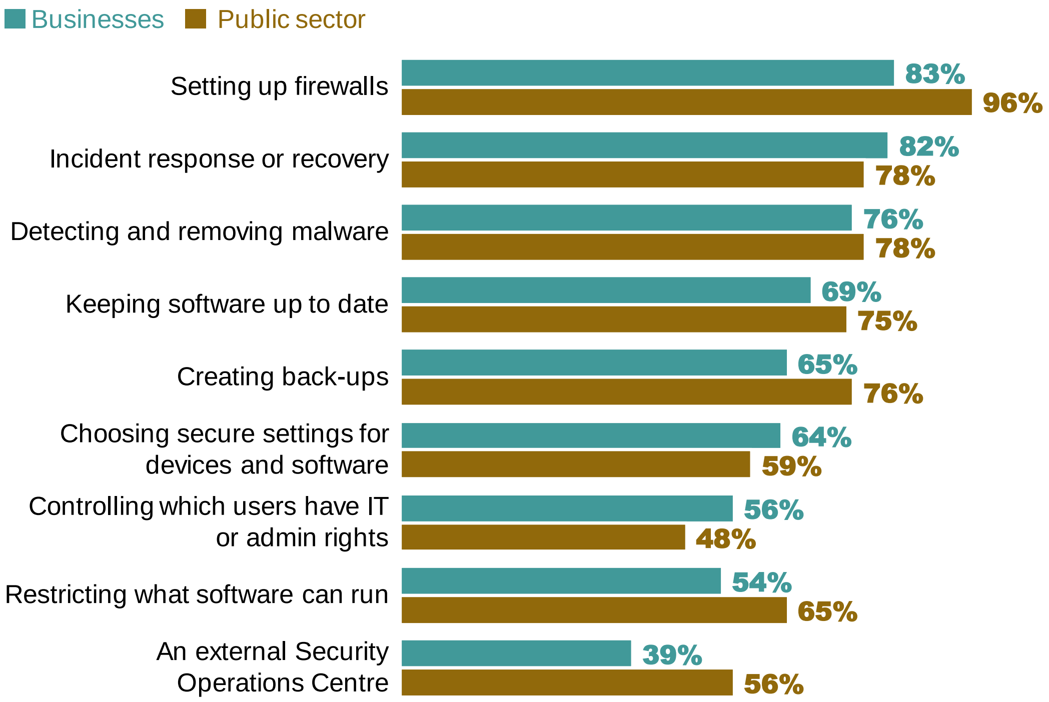
Outsourcing basic functions

Figure 8.2 shows the kinds of basic functions (as opposed to the more advanced functions covered in the next section) that get outsourced, among the organisations that outsource any aspects. There are too few charities that outsource cyber security in the sample to analyse for this question.

Setting up firewalls, incident response and detecting malware are the 3 most commonly outsourced functions in this list, with around 8 in 10 of those that outsource any aspects of cyber security incorporating these functions into this service. These results are very similar to the 2020 survey.[16] The functions that tend to be less commonly outsourced are around restricting software access and controlling admin rights.

Among those that outsource, a total of 31 per cent of businesses and 46 per cent of public sector organisations pass responsibility for all the functions mentioned in Figure 9.2 to their external cyber security providers. This highlights that most businesses still expect to perform various aspects of cyber security in-house, even if they use external providers.

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



Bases: 432 businesses that outsource cyber security; 40 public sector organisations that outsource cyber security

Outsourcing more advanced functions

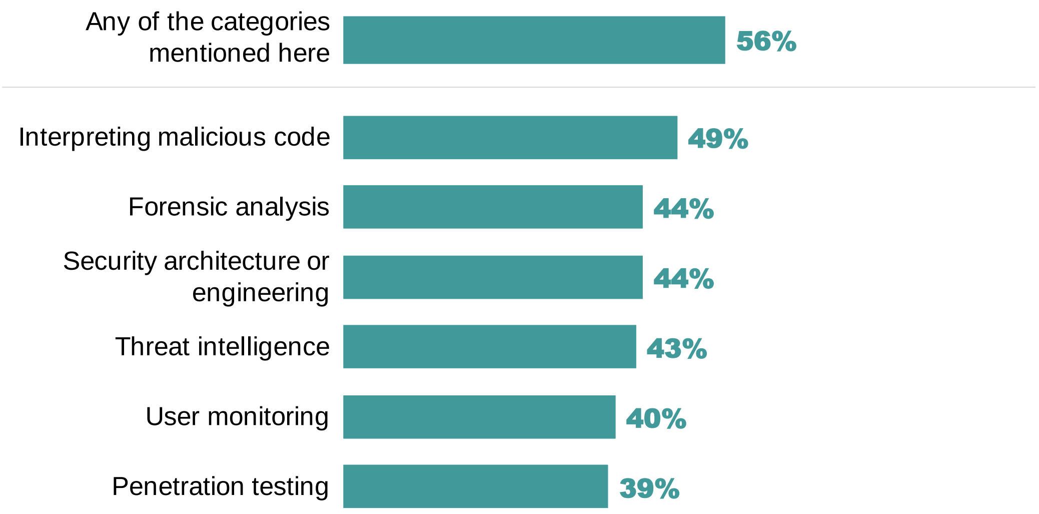
This year, we asked about external Security Operations Centres (SOCs) for the first time. External SOCs tend to be more common in public sector organisations (56% of those outsourcing) than private sector ones (39% of those outsourcing).

[16] In this year's survey, we reworded "dealing with cyberattacks" from the 2020 survey as "incident response or recovery", which is a more common term. Therefore, the results are not directly comparable, but have not significantly changed across years.

Figure 8.3 shows the other kinds of advanced functions that get outsourced, among the 38 per cent of businesses that outsource any aspects of cyber security. This reflects 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 2018 study). There are too few public sector organisations and charities in our sample to analyse for this question.

There is a broadly even spread in terms of these 6 tasks. The most likely to be part of the outsourcing relationship is interpreting malicious code. User monitoring and penetration testing are the least likely of these 6 areas to be outsourced.

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



Bases: 432 businesses that outsource cyber security; 40 public sector organisations that outsource cyber security

10 Conclusions and recommendations

Cyber security skills gaps and skills shortages continue to pose a major challenge for UK organisations, both within and outside the cyber sector. This year's labour market study reinforces the evidence from previous years on topics such as training, recruitment and workforce diversity. It also looks at new areas, including internships, staff turnover, and the role of recruitment agents and HR staff.

Our fieldwork took place in the shadow of the COVID-19 pandemic. This has created new, ongoing and unpredictable challenges in terms of increased workloads and risks of burnout in cyber teams, and the need for effective ways to train staff and share knowledge virtually. However, it has also created opportunities for engaging senior managers around cyber security, finding skilled individuals in the recruitment pool and more geographically diverse recruitment.

It should be noted that our survey findings are generally very consistent with the 2020 labour market study. Nevertheless, there is evidence of improvement in some areas, both in cyber sector businesses and the wider economy:

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

The rest of this chapter lays out the most important broad themes emerging from the 2021 study and our recommendations off the back of these findings:

- **Demand for cyber security staff dipped after the first COVID-19 lockdown but is now back to pre-pandemic levels.** While online job postings for core cyber roles fell by around a third between March and April 2020, the volume of job postings had fully recovered by Autumn 2020. The pandemic may have also led to a wider geographical spread of cyber security jobs, due to the increase in home working. In our qualitative research, recruitment agents and employers also expected applications from non-local candidates to increase

- **Across the wider economy, it is still common to find skills gaps in basic technical areas, as well as more advanced areas.** Half of UK businesses have a basic skills gap, lacking the confidence to carry out the kinds of basic cyber security tasks covered in the government-endorsed Cyber Essentials scheme. A third have more advanced technical skills gaps, with skills in penetration testing, forensic analysis and security architecture being most commonly mentioned. This highlights the ongoing importance of promoting basic cyber security guidance to businesses

- **Outside the cyber sector, cyber security is still felt to be misunderstood by management boards and, in some cases, within IT teams.** The lack of appreciation for cyber security among senior managers can lead to a poor cyber security culture among wider staff, a lack of investment in cyber security skills and training, and poor retention of staff in cyber roles. On the flipside, cyber leads want to know how to effectively influence senior managers, and the culture of the organisations they work for. This goes beyond simply having good communication skills, into skills around influencing behaviour and being able to frame discussions in terms of business risk

- **Outside the cyber sector, there is still a low awareness of training and career pathways.** In cases where businesses are providing training for employees in cyber roles, half think this training meets their needs only a fair amount, or not very much (as opposed to a great deal, or completely). Across both the job vacancies analysis and the qualitative findings, there also continues to be a high level of reliance on the same, narrow set of qualifications and certifications. There may be scope to promote more efficient or innovative training pathways, particularly for staff in IT roles. These staff have often had to maintain cyber security in their organisations during the rush to remote working, as a result of COVID-19

- **Job postings for cyber roles are widely regarded to be unrealistic in terms of their requirements.** The sense from the recruitment agents we interviewed was that, outside the cyber sector, the hiring managers who write job descriptions for cyber roles do not understand the labour market very well. This leads to them putting in unrealistic or unachievable criteria, potentially trying to recruit for 2 or 3 jobs in one. This not only leads to unfilled vacancies but also has implications for workforce diversity. Individuals aiming to work in cyber roles may become disillusioned and not apply. This was felt to disproportionately affect women and ethnic minority candidates

- **Cyber leads, both in the cyber sector and the wider economy, continue to lack awareness of workforce diversity issues.** Employers often report that the lack of diversity among their cyber staff is due to a lack of applications from diverse groups, while at the same time being unaware of their own stereotyping and potentially biased recruitment practices. In the cyber sector, workforce diversity is a consistent problem at all levels, but the reliance on recruiting senior positions from networks potentially makes this a tougher problem to solve at senior levels

- **In larger firms, the relationships between hiring managers, HR staff and recruitment agents are sometimes hampered by a lack of communication.** We heard positive examples where HR staff had been involved throughout the recruitment process, but equally cases where their involvement was an afterthought. Recruitment agencies were often used grudgingly, and this relationship could be very transactional. With more communication between these groups, recruitment agents and HR staff could help educate hiring managers on diversity issues and widen their recruitment approaches

- **Smaller cyber sector firms may have greater structural barriers to addressing skills gaps and skills shortages.** Large businesses in the cyber sector continue to disproportionately take on graduates and apprentices, in comparison to smaller firms. In the qualitative research, larger cyber firms also tended to have more structured training programmes and to have access to a wider range of recruitment methods. Employing career starters can bring unique benefits, but some firms may consider themselves too small for this. Therefore, there may need to be new ways for smaller cyber firms to broaden their recruitment and employ entry-level staff sustainably

The findings from this research should be viewed in tandem with the related DCMS study on the cyber security recruitment pool (2021), which looks at the same issues from a supply side perspective. It raises similar challenges around broadening recruitment approaches and career pathways, better segmentation of roles, unrealistic job adverts and workforce diversity. It also has its own set of recommendations to address these issues from the supply side.

Recommendations

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

We have opted not to simply repeat any of the 15 recommendations from the previous labour market study, instead producing a smaller set of new recommendations this year. However, given the consistency of the findings across years, the previous recommendations still stand, and government and industry should continue their efforts in these areas.

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

Changing attitudes and behaviours

Recommendation 1: The existing NCSC guidance for communicating cyber security risks to board members should be reviewed and, if necessary, updated and further promoted to ensure it helps cyber leads frame discussions in terms of commercial risk.[17]

Recommendation 2: There should be further guidance (e.g. on awareness raising and training activities), access to best practice and solutions for cyber leads on what works to change and maintain the behaviour of wider staff (outside of cyber teams) when it comes to cyber security.

Recommendation 3: The ability to positively influence the behaviour and culture within organisations should be included as part of the overall skills requirement for any Chartered Cyber Professional. These skills should also be included in the Qualifications Framework to be developed by the UK Cyber Security Council.

Career pathways and transitions

Recommendation 4: The ongoing work to map cyber security career pathways should include the development of example job descriptions and suggested minimum qualifications requirements for typical roles, to encourage cyber employers to draft more realistic job adverts.

Recommendation 5: The upcoming Career Pathways Framework for cyber security should include a set of training pathways or other innovative solutions that can quickly enable staff in a range of IT roles to gain essential cyber security skills or transition into cyber specialist roles. These solutions should be rolled out and promoted as soon as possible, potentially ahead of the overall Framework.

Recruitment and workforce diversity

Recommendation 6: Smaller businesses in the cyber sector should be encouraged and supported to build relationships with schools, colleges and universities in order to run work placements and internships, for example through a dedicated website or exchange scheme. This should enable them to take on more entry-level staff in cyber roles and carry out recruitment beyond their existing networks.

Recommendation 7: There should be written guidance or training materials targeted at cyber leads from small organisations – especially those that lack HR support – informing them of the basic actions

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

they could take to improve diversity. This includes, for example, things like writing neutral job adverts and making working environments suitable for neurodivergent employees.

Recommendation 8: Recruitment agents and HR staff should play a bigger role in educating cyber leads on good practice for realistic and unbiased recruitment. This might include, for example, events or workshops at cyber security conferences led by recruitment agents or HR professionals.

Recommendation 9: There should be further work to understand how to tackle diversity in senior roles within cyber sector firms – an issue which potentially extends into senior cyber roles outside the sector – and the steps that would improve career progression into these senior roles for diverse groups.

Our standards and accreditations

Ipsos MORI's 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 MORI was the first company in the world to gain this accreditation.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI 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 MORI 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 MORI 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 MORI 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 MORI 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-mori.com
http://twitter.com/IpsosMORI

About Ipsos MORI Public Affairs

Ipsos MORI 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.

Ipsos MORI Ipsos