March 2020

Cyber security skills in the UK labour market 2020

Findings report

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

Department for
Digital, Culture
Media & Sport

Ipsos MORI

Ipsos

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 & 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 training providers, cyber firms and large organisations in various sectors
- A secondary analysis of cyber security job postings on the Burning Glass Technologies database

Skills gaps

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

- Approximately 653,000 businesses (48%) 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[1], and are not getting support from external cyber security providers. The most common of these skills gaps are in setting up configured firewalls, storing or transferring personal data, and detecting and removing malware
- Approximately 408,000 businesses (30%) have more advanced skills gaps, in areas such as penetration testing, forensic analysis and security architecture
- A quarter (27%) have a skills gap when it comes to incident response (and do not outsource this)

Skills gaps are also common in the cyber sector. This extends to both technical and non-technical skills.

- Two-thirds (64%) of cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants. A quarter (25%) say that such skills gaps have prevented them *to a great extent* from achieving business goals
- Technical skills gaps are relatively high in each of the following areas: threat assessment or information risk management; assurance, audits, compliance or testing; cyber security research; implementing secure systems; and governance and management
- A total of 3 in 10 cyber firms (29%) also say that job applicants lacking non-technical skills such as communication, leadership or management skills has prevented them *to some extent* from meeting their business goals, and a similar proportion (28%) say this about their existing employees

Qualifications and training

The cyber sector workforce has a plethora of different qualifications and accreditations, highlighting a high level of fragmentation in the market for cyber security qualifications.

- Three-fifths of cyber firms (62%) report employing staff who have, or are working towards, cyber security-related qualifications (i.e. higher education, apprenticeships or other certified training)
- The most common technical qualification is the Certified Information Systems Security Professional (CISSP) accreditation, although only a fifth (19%) of cyber firms have any CISSP-accredited staff

[1] See https://www.cyberessentials.ncsc.gov.uk/advice/.

It is not common for businesses overall to invest in training for staff in cyber roles (24% have done so). However, this is much more common in medium firms (57%), large firms (59%) and, as might be expected, cyber sector businesses (73%).

In the qualitative interviews, the heads of cyber teams highlighted many challenges around identifying good quality courses and other accredited training for those in cyber roles:

- The fast evolving nature of cyber security means that university syllabuses constantly need refreshing. There was a desire for longer work placements to be integrated into degree courses
- There was a sense that the quality of vendor-specific accredited training could vary greatly. Cyber firms often needed to spend considerable time researching the available training options
- The importance of implementation skills – being able to implement technical knowledge in a business context – was frequently mentioned. Interviewees often felt that the current set of qualifications (both academic and technical) did not emphasise this element enough

Recruitment and skills shortages

Around 7 in 10 cyber sector businesses (68%) have tried to recruit someone in a cyber role within the last 3 years. These employers reported a third (35%) of their vacancies as being hard to fill.

- In 43 per cent of cases, this was because applicants lacked technical skills or knowledge. However, applicants lacking soft skills (22%) was also a common contributing factor
- In half (51%) of cases, employers have found it hard to fill generalist cyber roles
- Hard-to-fill vacancies are most commonly for senior level staff (with 3 to 5 years of experience) and principal level staff (with 6 to 9 years of experience)

We identified a total of 393,257 cyber security-related job postings over the past 3 years. Of these, 105,194 are formally labelled as cyber security jobs. The remaining 288,063 are cyber-enabled jobs, which include some cyber security functions among other job duties (e.g. network engineers whose role includes, but is broader than, network security).

- This analysis highlights geographic hotspots of activity in the cyber security labour market. These hotspots include London, Edinburgh and Belfast, as well as parts of the West Midlands and the South West, such as Bristol, Cheltenham and wider Gloucestershire
- The most common roles in demand are security engineers (18%), security analysts (13%), security architects (10%), security managers (9%) and security consultants (8%)
- The sectors most in demand of cyber talent are the finance and insurance, information and communications, and professional services sectors
- The technical skills areas most in demand include network engineering, risk management and technical controls, operating systems and virtualisation, cryptography and programming

The qualitative research uncovered further issues that organisations face when recruiting for cyber roles:

- High salary demands were commonly raised as a challenge. High wage differentials by sector and between London and the rest of the UK exacerbated this
- There were concerns about people frequently applying for roles that they did not have the skills or experience to perform, and exaggerating their expertise and experience in CVs
- Some cyber team heads found it difficult to align the job descriptions they were writing to particular qualifications. Some also felt that existing roles frameworks did not map well to qualifications

Diversity

The cyber sector workforce is not diverse. On gender diversity, it falls behind other digital sectors. Relatively few firms have adapted their recruitment processes or carried out any specific activities to encourage applications from diverse groups.

- 15 per cent of the workforce are female (vs. 28% of the wider digital sector)
- 16 per cent come from ethnic minority backgrounds (vs. 17% of the digital sector)
- 9 per cent are neurodivergent (for which no reliable comparisons are available)

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

- While diversity is largely viewed as a topic of increasing importance, there are still pockets of scepticism. Some interviewees felt it was overemphasised or no worse than in other digital sectors
- A more diverse workforce was rarely viewed as a way to tackle skills gaps and skills shortages in cyber roles. Instead, interviewees often focused on more nonspecific benefits
- There is a lack of awareness of neurodiversity in particular

Changes over time

This study builds on comparable labour market research conducted for DCMS in 2018. With roughly a year's gap between the two studies, we would not expect to see any major changes over this time. In general, the findings are very consistent. Nevertheless, there are small improvements across the business population.

- Fewer businesses have basic technical skills gaps (down from 54% to 48%)
- There is an increase in the proportion of businesses that have carried out a formal analysis of their cyber security training needs (from 14% to 22%)
- More businesses now consider it essential to have incident response skills (17% to 23%)

Conclusions

This study has raised several new insights into the individuals working in and applying for cyber roles, the skills gaps and skills shortages that affect employers, and the challenges that organisations face when it comes to training and recruitment. The main lessons we draw are as follows:

- Skills gaps and skills shortages continue to affect a large number of organisations. There needs to be more investment in technical skills and training, within the cyber sector and the wider economy
- Schools, universities and training providers need to give young people and training recipients a holistic skillset, covering the relevant technical skills and soft skills that employers demand, and the ability to implement those skills in a business context
- The cyber security labour market is challenging to navigate. Employers, recruitment agencies and job applicants may benefit from further guidance on career pathways, qualifications and training
- Many employers could benefit from broadening their recruitment practices, to employ more career starters, apprentices, graduates, people transitioning from other sectors or roles outside cyber security, and those from diverse groups

Contents

1 Introduction

1.1 About this research

The UK Government Department for Digital, Culture, Media & Sport (DCMS) commissioned Ipsos MORI, in association with Perspective Economics and Professor Steven Furnell from the University of Plymouth, to conduct research to improve their understanding of the current UK cyber security labour market. The work builds on comparable labour market research which Ipsos MORI conducted for DCMS in 2018 (roughly a year before this latest study).[2] It will inform the evidence base for government policy interventions to increase the UK's cyber security capability.

The research aimed to gather evidence on:

- Current cyber security skills gaps (i.e. where existing employees or job applicants for cyber roles lack particular skills)
- Current skills shortages and the level and type of job roles they affect (i.e. a shortfall in the number of skilled individuals working in or applying for cyber roles)
- 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
- The types of cyber security training products and services available, and whether these are meeting industry needs

It also aims to create a set of recommendations 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 6 strands, as outlined here. The role of the first 2 strands was mainly to feed into the development of the quantitative survey (strand 3) and qualitative research (strand 4), by scoping out the gaps in the existing literature and the topics that should be explored.

1. **Methodology and evidence review –** Professor Steven Furnell from the University of Plymouth carried out a rapid evidence review looking at the existing literature on cyber security skills gaps and shortages. The Ipsos MORI team and our academic partners on the study (see acknowledgements section in this chapter) also reviewed the questionnaire from the 2018 research. We carried out this work across June and July 2019.

2. **Training provider market scoping –** Ipsos MORI and Perspective Economics carried out 7 in-depth interviews with cyber security training providers. Perspective Economics also carried out a review of all the UK training provider websites to give an overview of the market and help categorise the products and services being offered. This took place from June to August 2019.

3. **Quantitative surveys –** Ipsos MORI conducted 1,558 telephone surveys with 4 audiences: general businesses (1,046), public sector organisations (106), charities (201) and cyber sector

[2] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market.

firms (205). Fieldwork was between 7 August and 8 October 2019. The survey data is weighted to be representative of the population profiles of these respective audiences. The business sample excludes agriculture, forestry and fishing businesses. The public sector sample excludes parish councils and central government departments.[3]

4. **Qualitative interviews** – Ipsos MORI conducted a more focused strand of qualitative research, with 23 in-depth interviews split across 15 large organisations and 8 cyber sector firms. Interviews took place across September 2019.

5. **Job vacancies analysis** – Perspective Economics analysed 393,257 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 covered vacancies over a period of 3 years, from September 2016 to the end of August 2019.

6. **Recommendations workshop** – Ipsos MORI ran 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 2019.

The separately published technical report provides more detail on the methodology, including sampling, data collection, response rates and weighting.[4] It also includes a copy of the strand 1 literature review as an appendix.

This findings report focuses on the picture in the UK. As part of the strand 1 evidence review, we also explored other nations' approaches to filling cyber security skills gaps, and this is also included in the technical report appendix.

1.3 Similarities and differences from the 2018 labour market study

For the survey of general businesses, charities and public sector organisations, the methodology is the same as in the 2018 study. These survey findings are intended to be comparable across years, where the same questions have been asked to the same groups.

However, there are various differences in the methodology this year, which affect the nature of the findings pulled out in this report. We summarise the main differences below:

- Strands 2 (training provider market scoping), 5 (job vacancies analysis) and 6 (recommendations workshop) are entirely new for this year
- In the quantitative survey, cyber sector firms were included as a sampled group for the first time this year. We have also included findings from a separate, comparable survey of the same group carried out as part of the DCMS Cyber Sectoral Analysis 2020.[5] Fieldwork for this survey was carried out in summer 2019

[3] We considered organisations with no IT capacity or online presence as ineligible, which led us to exclude a small number of specific sectors (agriculture, forestry and fishing). We would typically have screened such organisations out of the survey, so we excluded them from the sample instead. This matches the approach taken in DCMS's Cyber Security Breaches Survey series. We excluded parish councils, which also tend to have little or no IT capacity. If included, the volume of parish councils means that the public sector sample would have been dominated just by these. Finally, in agreement with DCMS, we ensured that central government departments were not on the sample, as we anticipated they would not be able to take part or share sensitive information.

[4] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020.

[5] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020. We include a full set of references and links to all external reports at the end of this report.

- In the quantitative survey, the sample size for charities is lower this year (201) than in 2018 (470). The margins of error for the charity findings this year are consequently higher. They were ±4-6 percentage points (accounting for weighting) in 2018 and are ±6-10 percentage points this year
- The qualitative strand focused on a different audience this year. In 2018, it followed up a range of organisations that took part in the quantitative survey, of all sizes and sectors. This year, we focused on large organisations and cyber sector firms

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

Other well known surveys have been published since the 2018 DCMS study, including:

- The ISC2 2019 Cybersecurity Workforce Study[6]
- The EY Global Information Security Survey 2018-19[7]
- The ISACA State of Cybersecurity 2019[8]

These surveys often yield results that paint a very different picture of cyber security skills gaps and shortages. There are important methodological differences between these surveys and our DCMS study, which help to explain some of these differences:

- 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. The above surveys have 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 above surveys 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 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 in a particular way – we ask whether those in cyber roles within organisations are confident that they or people in their team can carry out a range of cyber security tasks involving specialist skills. This does not objectively test whether these organisations possess these skills, but the task based approach is more reliable than other surveys that simply ask organisations to self-report any specific skills gaps they have

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.

[6] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study.
[7] See https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf.
[8] See https://cybersecurity.isaca.org/state-of-cybersecurity.

In stacked bar charts with bars showing values under 3 per cent (Figures 2.7, 4.3, 4.5, 5.1 and 5.5), 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. There are too few public sector organisations and charities sampled to split out results by size or income.

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.[9] 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 5, 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). Similarly, where

[9] See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

we indicate that findings have changed since the 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 or insight 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.

Approach to references and footnotes in this report

We often reference the same external reports or sources more than once within a chapter. In these cases, the first mention in the chapter receives a footnote and subsequent mentions are cross-referenced to this same footnote (rather than getting a new footnote).

1.6 Acknowledgements

The authors would like to thank all the businesses, charities and public sector organisations, and the individual research participants who took part in the survey and interviews. We would also like to thank the following partners who also contributed at various stages to the study:

- Professor Mark Button, Institute for Criminal Justice Studies, University of Portsmouth
- Professor Andrew Martin, University of Oxford
- Dr Victoria Wang, Institute for Criminal Justice Studies, University of Portsmouth

Finally, we would 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 job titles, career pathways into the role and the qualifications they hold.

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

The wider context from external literature

- DCMS's Cyber Sectoral Analysis 2020 estimates 42,855 full-time employees working in cyber roles in the UK cyber sector, across the 1,221 cyber security companies that make up this sector.[10] This excludes individuals working in cyber roles outside of these companies
- The 2019 ISC2 Cybersecurity Workforce Study, a global online study of IT and cyber professionals, estimates that there are c.289,000 people employed in cyber roles in the UK, across all sectors[11]
- The same ISC2 study also found that unclear career pathways and the cost of cyber security certifications were barriers to career progression among cyber professionals
- The existing literature tends to focus more on those working professionally in cyber roles. There is much less coverage of organisations where cyber functions are carried out informally

2.1 Size of cyber teams

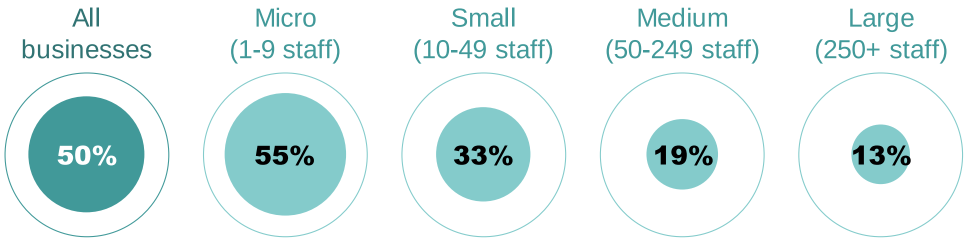
Cyber teams outside the cyber sector

Outside the cyber sector, organisations' in-house cyber teams are typically very small. Half (50%) of all businesses have just one person managing or running cyber security in-house. This is lower for charities (32%) and public sector organisations (25%), suggesting they are slightly better resourced.

The size of cyber teams is linked to the staff size of the organisation, much more strongly than to other characteristics such as financial turnover. As Figure 2.1 shows, larger businesses are less likely to have just one employee covering cyber security functions. However, even among large businesses, the typical (median) cyber team comprises just 2 to 3 people.

[10] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020.
[11] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study.

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



Bases: 1,046 businesses; 556 micro; 260 small; 132 medium; 98 large

Finance and insurance businesses also tend to employ slightly more people in cyber roles than average, but again the typical (median) finance or insurance business has just 2 to 3 people in these roles.

The businesses that outsource aspects of their cyber security tend to also have slightly larger in-house cyber teams (57% have more than one person in the team, vs. 41% of those that do not outsource). This suggests that outsourcing is more commonly used as a way of strengthening existing in-house teams, rather than to make up for the absence of in-house cyber security staff. Broadly speaking, it is being used to address skills *gaps* (a lack of skills) rather than skills *shortages* (a lack of people).

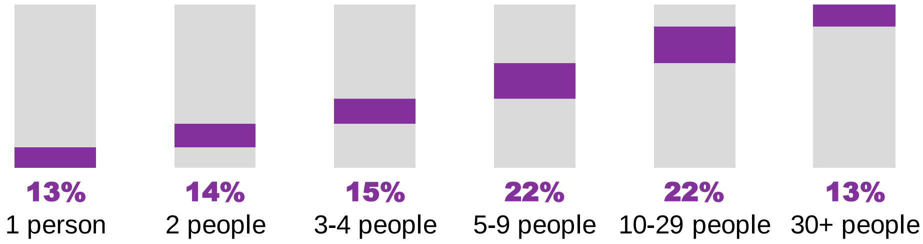
The 2018 survey also indicated that cyber teams in the wider economy tend to be very small. However, this year, a higher proportion of public sector organisations have just one staff member working on cyber security (25%, vs. 12% in 2018), indicating that they are less well staffed than before.

Cyber teams within the cyber sector

Most firms in the UK cyber sector (i.e. those trading in cyber security products or services) are smaller businesses. The DCMS Cyber Sectoral Analysis 2020 estimates that 55 per cent are micro (1 to 9 staff) and 23 per cent are small (10 to 49 staff).[10] Reflecting this, our survey finds that the typical (median) cyber team within these businesses consists of 6 people.

The full picture is shown in Figure 2.2. It shows that a quarter of cyber firms (26%) are especially small, operating with just 1 to 2 employees in cyber roles. 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



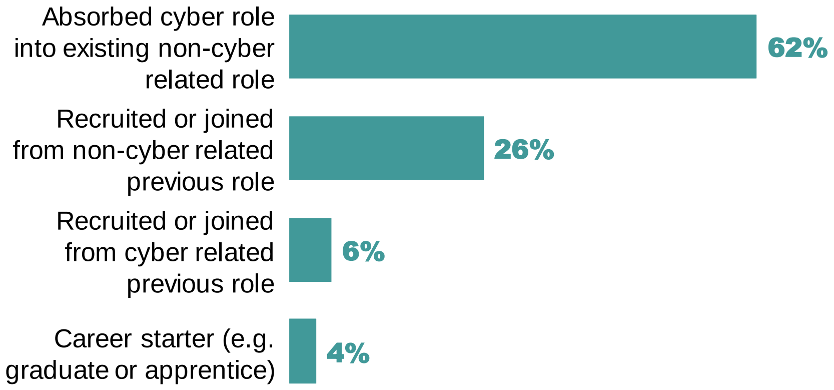
Base: 205 cyber sector businesses

2.2 Career pathways into cyber roles

Career pathways into cyber roles outside the cyber sector

Outside the cyber sector, the majority of staff working in cyber roles in private businesses have absorbed these roles into an existing non-cyber role. Figure 2.3 shows the full data for private businesses.[12]

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



Bases: c.970 businesses (where answers given on team size and on how each individual came into the team)

These findings are broadly in line with the 2018 results. They highlight, as we found in 2018, that many private sector firms do not treat cyber security as a single job and expect the responsible staff members to carry out cyber security functions alongside their existing job roles.

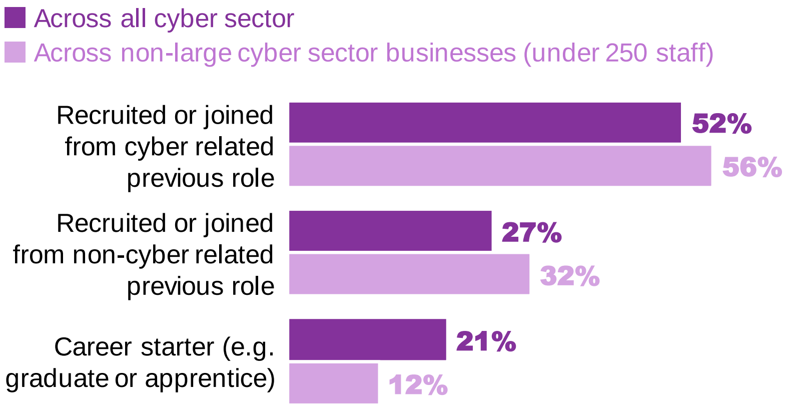
Career pathways within the cyber sector

As Figure 2.4 shows, around half (52%) of the cyber sector workforce have entered their current roles after a previous role in cyber security. Relatively few joined as career starters (21%).

Moreover, when excluding the large businesses from our cyber sector sample, the proportion joining as career starters drops to 12 per cent. This highlights that, outside the small number of larger businesses in this sector, very few appear to be offering graduate schemes or other entry level positions (a theme we return to in Chapter 6 when discussing recruitment).

[12] There are too few charities and public sector organisations sampled this year to estimate the cyber workforce distribution for these organisations.

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



Bases: 188 cyber sector businesses (excluding those that could not break down their workforce); 185 non-large cyber sector businesses (under 250 staff)

Perceptions of apprenticeships (cyber apprenticeships and other apprenticeships)

The qualitative research suggests a generally positive attitude towards apprenticeships in cyber teams. Where discussed, the heads of cyber teams saw them as good opportunities to fill skills gaps. Various benefits were mentioned, including allowing people with no cyber security background to enter the profession, getting staff who do not have preconceptions about working in cyber security and staff who sometimes have better soft skills than those coming through the university route.

Those we spoke to also appreciated that apprentices are not job ready. They expected, to a certain extent, mixed levels of maturity and mixed success when taking them on.

However, there were cases where firms had struggled to find apprentices or found it challenging to match them up with the right training courses for their specific cyber roles. Some wanted to see more flexible and broader apprenticeship frameworks and standards covering a wider range of technical cyber security skills, so that more cyber roles could be filled by apprentices.

Various interviewees said they had a long term aspiration to offer apprenticeships but felt that they could not do this until they had a more established team. The same reasoning was also used for not taking on graduates as well. One of the perceived barriers was a sense that they would not have the time to train up apprentices or other new joiners. This meant that, even though they were positive about the concept, they were not willing to take on apprentices until after they had more experienced staff on board.

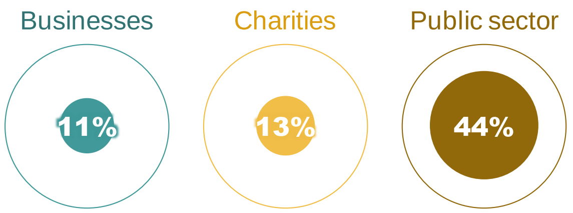
2.3 Are cyber roles labelled as such across UK organisations?

We know from the 2018 labour market study 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. This section quantifies these issues and focuses on the survey of general organisations, rather than cyber sector businesses.

Formal versus informal roles as written into job descriptions

As Figure 2.5 highlights, the vast majority of organisations continue to have staff performing cyber roles informally rather than as a recognised cyber professional. These findings are similar to the 2018 survey.

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



Bases: 1,046 businesses; 201 charities; 106 public sector organisations

In the private sector, a higher proportion of medium (34%) and large businesses (24%) have the cyber role written into job descriptions. This is also more common in the finance and insurance sectors (32%, vs. 11% overall), information and communications (19%) and health, social care and social work sectors (18%). However, it is worth noting that even in these size and sector subgroups, most businesses still do not have individuals with formal cyber security responsibilities as part of their job descriptions.

Job titles of those carrying out cyber functions

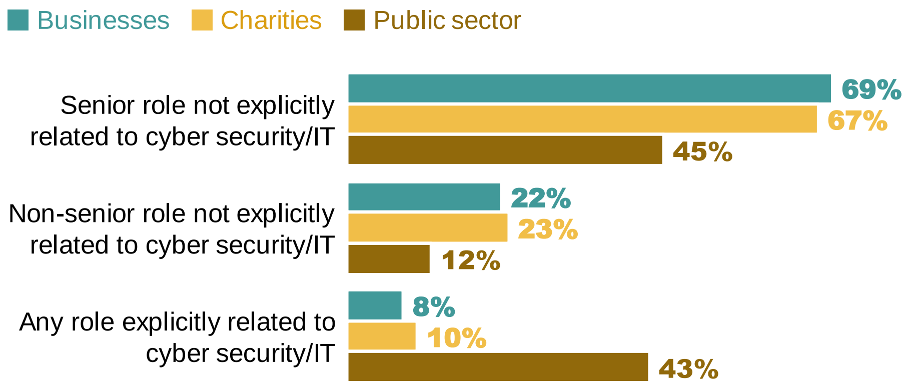
This is a new question for 2020. It highlights that, across the private sector, the vast majority of people performing cyber functions are not in cyber security-focused job roles, or even in IT roles. In 9 in 10 businesses (91%), the individual most responsible for carrying out cyber security functions is not working in a role focused on cyber security or IT. In 7 in 10 businesses (69%), it is another senior individual such as a Director, while in 2 in 10 cases (22%), it is a non-senior colleague such as an Office Manager or someone in an assistant role. The summarised breakdown is in Figure 2.6.

This is largely driven by the size of the business. In 92 per cent of micro or small businesses, the individual responsible for cyber security functions has a wider job role outside cyber security or IT. In two-fifths of these businesses (39%), the responsible individual is the business owner, Chief Executive or Managing Director. However, even in most medium businesses (64%) and half of large businesses (51%), the responsible individual is not in a cyber security-focused job role or an IT role.

Even in businesses where cyber security functions are formally written into job descriptions, job titles tend not to be cyber security or IT-focused (in 80% of cases). This highlights the extent to which people seem to be sharing the cyber security role with other workplace responsibilities.

Figure 2.6 also shows that charities are largely similar to businesses in this regard. Public sector organisations are much more likely to have people with cyber security or IT-related job titles (43%).

Figure 2.6: Percentage of organisations where the individual most responsible for cyber security falls into the following categories (based on their job title)



Bases: 1,046 businesses; 201 charities; 106 public sector organisations

There is also very little commonality in cyber security job titles across businesses (which also reflects the wider research literature noted at the beginning of this chapter). Just 6 per cent of large businesses employ a Head of Information Security (or Cyber Security), 5 per cent have a Chief Information Officer and 1 per cent have a Chief Information Security Officer (CISO). Across businesses of all sizes, these positions make up less than 1 per cent of those ultimately responsible for the business's cyber security.

Departmental positions of those carrying out cyber functions

The 2020 survey also looks for the first time at the department that the individuals responsible for cyber security sit in. This highlights that few businesses have specific cyber security departments or teams (1% of all businesses and 7% of large businesses do). Instead, these functions often do not sit in a specific team at all. Where they do, this is typically with IT or finance teams.

Most commonly in the private sector, this position resides with individuals on management boards (38%). However, this is driven by business size, because in smaller businesses, it is more common for senior directors to take on responsibility for cyber security functions.

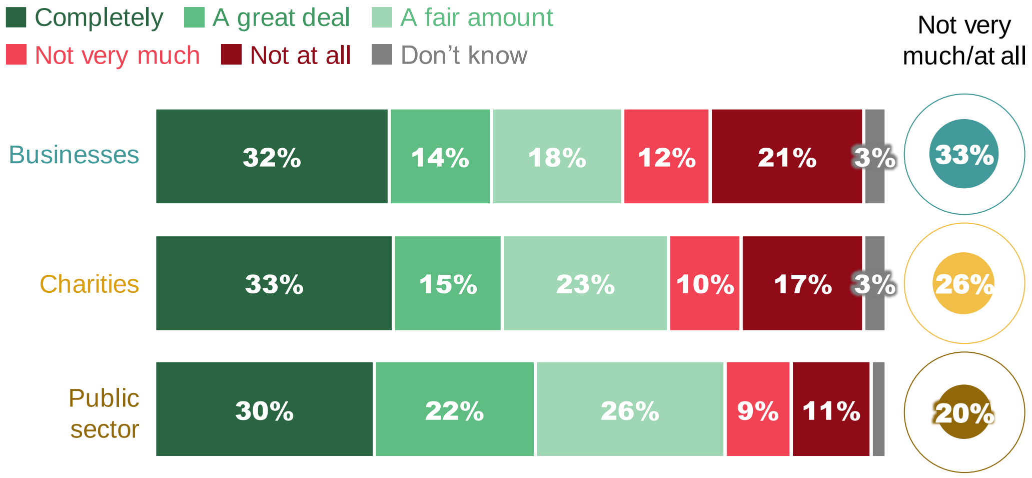
Looking solely at medium and large businesses, the individual ultimately responsible for cyber security is most commonly in the IT department (in 30% of medium businesses and 41% of large businesses). Outside of this, the next most common home is in finance departments (in 18% of medium businesses and 16% of large businesses). It is relatively uncommon for these individuals to sit in compliance or legal teams (in 2% or medium and large businesses respectively).

Covering cyber roles during absences

The 2018 survey raised the issue that organisations may be more exposed to cyber risks if there is only one individual working in cyber security, and there is no one else to cover this work in their absence. It could also mean that organisations inadvertently lose cyber security skills when those performing cyber security roles leave the organisation, and no one else takes on this role.

Figure 2.7 shows that a third of businesses (33%) and a quarter of charities (26%) are exposed to such risks, saying this role would not be covered very much, if at all, during absences. This is less the case for public sector organisations (20%).

Figure 2.7: Extent to which others in the organisation would have the skills and knowledge to cover cyber roles when the lead individual is absent



Bases: 1,046 businesses; 201 charities; 106 public sector organisations
Unlabelled bars are under 3%.

These findings are largely similar regardless of whether the cyber security role is written into job descriptions or not. This highlights the risk of staff shortages even in organisations that are taking a more considered approach to cyber security than the norm.

Geographically, this risk also appears to be higher for businesses in the North of England (39% not covered very much or at all) and the Midlands (43%) than for those in the South East (29%), London (25%) or Scotland (26%). There are too few sampled businesses in Northern Ireland or Wales to examine separately.

2.4 Qualifications for those in cyber roles

How many staff within cyber sector firms are qualified?

The 2018 survey established that it was relatively rare for those performing cyber functions in firms outside the cyber sector to have relevant qualifications or accreditations (i.e. qualifications their employer considered relevant to their role). Just 4 per cent of businesses had staff with any relevant qualification or accreditation, including any IT-related qualifications. This was 32 per cent among large businesses.[13]

As cyber roles continue to be assigned informally across many organisations, we do not expect these results to have changed since the previous survey. Therefore, this year's study focuses on qualifications among staff in cyber sector firms. These staff, working professionally in cyber roles, are expected to have the requisite technical knowledge for their jobs.

Three-fifths of cyber firms (62%) report employing staff who have, or are working towards, cyber security-related qualifications or certified training. However, this leaves two-fifths of cyber firms (38%) that do not employ any staff with such qualifications or certifications, or are unsure if their staff are qualified. This includes more generalist qualifications like computer science or IT degrees – the survey asks firms to specify what qualifications they are referring to, which we explore in the next section.

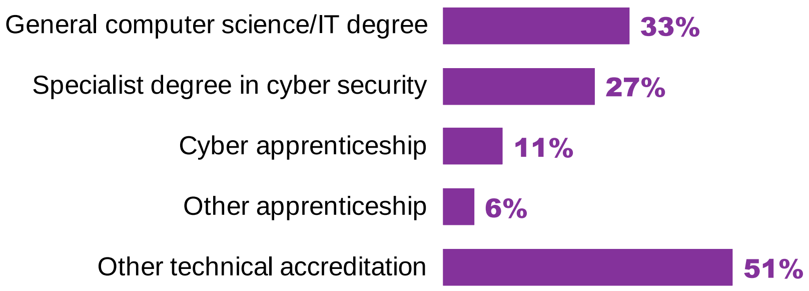
[13] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market.

Types of qualifications held in the cyber sector

The full breakdown in Figure 2.8 illustrates what cyber firms are referring to when they suggest their staff are qualified for working in cyber roles. These percentages are based on all cyber firms, not just the 62 per cent that say their staff have any relevant qualifications or accreditations.

It is more common for staff to hold degrees in computer science or IT than specialist cyber security degrees (33% vs. 27%). It is relatively rare for cyber sector firms to be using apprenticeship schemes. This ties in with the finding at Figure 2.4 and suggests that few firms are currently developing career starters, for example as apprentices.

Figure 2.8: Percentage of cyber sector firms that have staff with the following types of qualifications or accreditations



Base: 205 cyber sector businesses

Half (51%) have technical qualifications or accreditations other than degrees and apprenticeships. Among these 51 per cent, there are recurring mentions of:

- Certified Information Systems Security Professional, or CISSP (38%)
- Certified Information Security Manager, or CISM (14%)
- CREST-approved training (12%)
- Certified Ethical Hacker accreditation (12%)
- ISO 27001 Certified Information Security Management Systems, or ISMS (11%)

We recorded (without prompting) another 28 specific cyber security accreditations held by staff in cyber sector firms. This shows a high level of fragmentation in the market for cyber security certifications. This also emerged as a theme in the qualitative research and is something we discuss further at the end of this chapter.

Reflections on the pros and cons of the CISSP accreditation

The survey results show that CISSP is the most popular single cyber security accreditation in the cyber sector. Despite this, four-fifths (81%) of cyber sector businesses do not have any CISSP-accredited staff. Therefore, it is far from being an accepted baseline qualification for those working in cyber security.

The qualitative research provides further insights into why this might be. CISSP was often acknowledged in interviews to be one of the most widely recognised accreditations in the cyber sector. However, interviewees also flagged a shortage of CISSP-accredited individuals in the labour market.

One cyber team head linked this shortage to the fact that CISSP requires a minimum of 5 years of work experience, making it hard to obtain. Another noted that having it as a requirement in job adverts could potentially discourage new entrants into the labour market. As such, those with the CISSP qualification tend to have high wage demands, that often push them out of the reach of prospective employers. This was felt to be a bigger issue outside London, where salaries are typically lower.

The qualitative research suggests that increasing the number of CISSP-qualified individuals is important, but unlikely to be a solution on its own. For instance, the fact that it is a broad qualification that covers both the governance, regulation and compliance (GRC) aspects of cyber security as well as the technical aspects was felt to be an advantage – other qualifications do not tend to cover both areas. However, some interviewees also said that CISSP would not be sufficient for more specialised cyber roles and functions and may not be an appropriate baseline qualification for specialist roles.

"The gold standard is CISSP. It is a generalist certification, which is a mile wide but an inch deep. The fact that someone has passed that shows that they have a wide understanding of security and can hold a security conversation with a client."

Cyber sector business

Broader issues and challenges around cyber security qualifications

The qualitative research also raised several issues and challenges around the modernity of qualifications and their relevance in a commercial environment. It is worth noting that these are very similar to the themes raised in the earlier DCMS/Centre for Strategy & Evaluation Services report.[14] Our work reinforces many of the findings from that study.

- The fast evolving nature of cyber security means that the syllabuses for different qualifications risk becoming out of date. This was considered more of an issue for academic qualifications than for technical accreditations. PhDs and Masters degree courses in cyber security often lasted 3 years, leaving some heads of cyber teams concerned that some of the content may be irrelevant or outdated by the end of the course. One qualitative interviewee also noted that it was hard to find existing courses that dealt with new standards and processes such as the NIS Regulations[15]

- Interviewees also felt that the current set of qualifications (both academic and technical) often did not provide individuals with the ability to practically implement technical skills and knowledge in a business environment. For example, one cyber team head felt that the ISO 27001 Lead Auditor qualification teaches what an audit is, but it does not tell people about the practical challenges they will face carrying out an audit in a business

"We have a lot of people who have qualifications but have no clue what they are talking about."

Large organisation outside the cyber sector

- A potential driver of this implementation skills gap was the lack of good quality work placements being integrated into degree courses. For instance, one interviewee noted that long term placements of around 6 months were typically more successful than short placements lasting just 1 or 2 weeks, but they felt that long term placements were relatively uncommon. One interviewee from the cyber sector felt strongly that there was currently not enough of a reciprocal benefit for cyber sector employers that partnered with schools, colleges or universities, and that there might be better incentives to encourage such partnerships

[14] See https://www.gov.uk/government/publications/the-role-of-further-and-higher-education-in-cyber-security-skills.
[15] See https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018.

The challenge of having such a wide range of qualifications and accreditations was also highlighted:

- This made it challenging for some interviewees to know which qualifications were of good quality or right for a UK audience. For example, one interviewee mentioned the Global Industrial Cyber Security Professional (GICSP) qualification, which they felt to be high quality but focused on a US audience. The range of qualifications also made it expensive to pursue a career in cyber security, because job applicants would need to acquire multiple qualifications to improve their employability

- One interviewee felt that having a wide range of qualifications was inevitable, because it reflected the diversity of product vendors in cyber security and the need for vendor-specific qualifications. At the same time, some felt that the status of certain qualifications could be elevated, so these could be treated as gold standards. As an example, for interviewees in GRC roles, the ISO and Payment Card Industry (PCI) qualifications were considered as possible gold standards

- Providing more quality assurance for qualifications was considered as a potential area for government involvement. On this, one interviewee highlighted the helpfulness of the list of certified degrees on the National Cyber Security Centre (NCSC) website.[16] However, there was often a lack of awareness across interviewees of existing government work in this area, such as the NCSC Certified Cyber Professional (CCP) accreditation – in our quantitative survey, just 3 per cent of cyber sector firms have this qualification among their workforce[17]

"If the government could promote or endorse training, with a grading structure or criteria that people have to meet, that would be very good. If they could create a structure where private companies deliver the same quality of training, that would be really good."
Large organisation outside the cyber sector

In Chapter 6, we further discuss the relative importance of qualifications as a factor in recruitment. We also discuss in Chapter 3 how improving qualifications is likely to only partly address skills gaps, in terms of giving cyber security job applicants a more holistic skillset.

[16] See https://www.ncsc.gov.uk/information/ncsc-certified-degrees.
[17] See https://www.ncsc.gov.uk/information/about-certified-professional-scheme.

3 Diversity in cyber security

This chapter explores diversity in the cyber workforce, with a focus on gender, ethnicity and neurodiversity[18]. It covers how cyber team heads perceive and frame the issue of diversity and the actions they are taking to diversify their teams.

We also cover quantitative estimates of diversity across cyber sector businesses. Our estimates focus on these businesses and not the wider group of people working in cyber roles outside the sector. This reflects the fact that the vast majority of the wider workforce, outside the cyber sector, are performing cyber roles in an informal capacity. Including these individuals would provide a misleading picture of diversity within the cyber professional workforce.

The wider context from external literature

- The lack of gender diversity in the cyber security workforce is a global issue. Recent studies that have found a substantive skew towards men in the workforce include the 2019 ISC2 Cybersecurity Workforce Study[19] and the ISACA's State of Cybersecurity 2019[20]. Both these pieces of research focus mostly on very large global businesses
- It is also an issue in the UK, both in terms of the known professional workforce and the pipeline. The Chartered Institute of Information Security estimates that 9 per cent of its members are women.[21] A recent DCMS/Centre for Strategy & Evaluation Services report highlights that only 16 per cent of those taking cyber security degrees in 2016/17 were female.[22] However, these studies do not provide a representative estimate of diversity for the current UK cyber workforce
- The existing literature, where it covers diversity, tends to only address gender diversity. Ethnicity and neurodiversity have not been explored in the same fashion

3.1 Attitudes towards workforce diversity

The framing of diversity as an issue

In the qualitative interviews, a lack of diversity in cyber security was frequently, though not universally, accepted as an important issue to be tackled. Several cyber team heads acknowledged that their workforce was currently dominated by white males and that this was not reflective of wider society. They were often able to quote the statistics, especially around gender, for their own teams or companies. Many also agreed that more could be done to improve the diversity of the current labour market.

There was a broad sense of increasing importance in this issue, with conversations around it having stepped up in the last couple of years. In one case, this was linked to the clients of cyber sector businesses increasingly expecting greater diversity within suppliers, as their own organisations became more focused on the topic. It was also linked to the gender pay gap regulations introduced in 2017, which had prompted some organisations to review their diversity more broadly.

[18] 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).

[19] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study.

[20] See https://cybersecurity.isaca.org/state-of-cybersecurity.

[21] See https://www.ciisec.org/CIISEC/Resources/White_Papers/CIISEC/Resources/White_Papers.

[22] See https://www.gov.uk/government/publications/the-role-of-further-and-higher-education-in-cyber-security-skills.

"Diversity is increasingly important, and our clients expect it as well. Our clients are increasingly diverse."

Cyber sector business

However, there were also pockets of scepticism across the interviews. In rare cases, some felt that the problem was overemphasised or that the scale of the issue was in line with other digital sectors, and therefore should not have special treatment in the context of cyber security. These interviewees stressed that staff were recruited based on merit, and that this should always be the most important factor. These tended to be the organisations that were taking few or no concrete steps to improve their own cyber workforce diversity.

"When we would look to recruit, I don't think diversity would come into it. We would just look for the best person for the job."

Large organisation outside the cyber sector

Where it was seen as an important issue for organisations, there was commonly a greater focus on gender diversity over other aspects. Gender diversity was often mentioned without further prompting. There were still, to a lesser extent, spontaneous discussions of other aspects of diversity, including ethnicity, nationality, social class and sexual orientation. By contrast, it was relatively rare for interviewees to spontaneously discuss neurodiversity. In fact, there was a comparatively low awareness of this term, with some saying they had not considered this aspect of diversity at all.

Responsibility for diversity

There was a sense from some qualitative interviewees that, while diversity was important, it did not feel like something they could particularly control. They emphasised that it was a problem with the pool of applicants rather than with their recruitment approaches – they had not set out to recruit a nondiverse workforce, but it had naturally fallen out that way. For example, one interviewee emphasised that the CVs they received were overwhelmingly male, so they had less choice over who they could recruit.

"I can only pick from the CVs that are put in front of me."

Cyber sector business

In other cases, where ethnicity was discussed, a few based in less ethnically diverse areas said that their workforce was simply reflective of the local area.

The perceived benefits of having a diverse workforce

Typically, in the qualitative interviews a more diverse workforce was not viewed, directly, as a way to tackle skills gaps and skills shortages in cyber roles (by widening the pool of applicants). Instead, when probed about the rationale for diversifying cyber teams, team heads tended to focus on broader benefits. These were often nonspecific benefits that were not guaranteed, but they were still considered as important motivations to improve diversity:

- There was sometimes a sense that improving diversity was the right thing to do, for society generally as well as for business needs. For instance, one interviewee felt that a more diverse team would better reflect their clients and improve their client relationships

> ***"We look at diversity as something we should be doing because it is a good thing to be doing."***
> *Large organisation outside the cyber sector*

- A more diverse team was felt to improve organisational culture and to emphasise the positive values of the organisation. There was a view that it could create better working environments, raise employee wellbeing and retention, and attract new joiners by making the organisation stand out

> ***"It is easier to recruit as well when you have got a very obvious mixed diversity within your employee base."***
> *Large organisation outside the cyber sector*

- Several cyber team heads discussed how a more diverse workforce would bring new skills to their teams. However, these discussions typically focused on soft skills with relatively intangible benefits, rather than on technical cyber security skills. For instance, various interviewees felt that having more women in their teams could lead to improved empathy and team bonding. There were also mentions of women tending to have better communication or negotiation skills

> ***"Everyone brings something different to the table. It makes the meal at the end of the day much nicer."***
> *Large organisation outside the cyber sector*

- Finally, there was a sense that diverse cyber teams would benefit from new ways of thinking and problem solving, which could lead to greater productivity and innovation. For example, one interviewee highlighted that cyber teams needed to match the diversity of those carrying out cyberattacks, so that they could come up with better responses to such attacks. Some mentioned that an ethnically diverse workforce would bring a different cultural outlook on situations. In this context, interviewees also felt that a neurodiverse workforce would have very different approaches to problem solving that could benefit their organisation

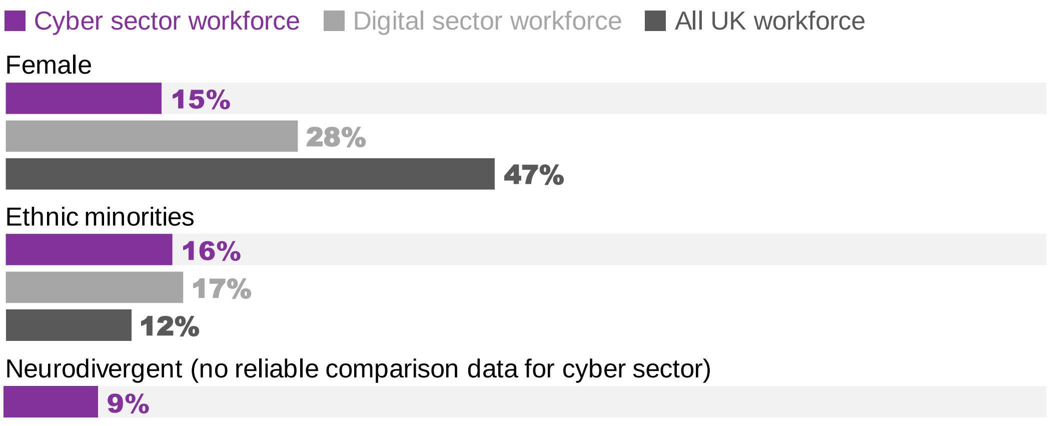
3.2 Estimates of diversity in the cyber sector

The quantitative survey results (Figure 3.1) show that the cyber sector is behind other digital sectors, and behind the UK economy as a whole, on gender diversity. We estimate just 15 per cent of the workforce to be female. On ethnic diversity, the cyber sector is in line with other digital sectors.

Around 1 in 11 of 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 this compares to other sectors or to the wider UK workforce. However, the Advisory, Conciliation and Arbitration Service (ACAS) website notes that 15 per cent of the population are neurodivergent.[23] This suggests that there is potential for the cyber sector to increase its neurodiversity.

[23] See the ACAS website, at https://www.acas.org.uk/neurodiversity.

Figure 3.1: Percentage of cyber sector workforce that come under the following diverse groups[24]



Bases: 198 cyber sector businesses for gender estimate; 183 for ethnicity estimate; 163 for neurodiversity estimate (excluding those that were not able to answer these questions, or refused)

3.3 Approaches taken to improve diversity

In the qualitative research, we sometimes found that the approaches taken to improve diversity were piecemeal and broad, as opposed to reflecting a cohesive strategy. Examples cited by interviewees included women-only events at conferences, women's forums within organisations, or having positive case studies on intranet pages. In some cases, individuals had taken part in or were aware of industry initiatives such as the Cyber Ready training programme (funded through the Cyber Security Skills Immediate Impact Fund)[25] and the Civil Service Positive Action Pathway. We also found various examples of changes to recruitment practices (discussed later in this section).

Where organisations were taking a wider range of actions on diversity, this often included having specific individuals focused on the issue. There were examples of diversity working groups, hired consultants and, in one case, an organisation having a head of diversity and inclusion in post.

One cyber firm exemplified this more comprehensive approach. They said that the majority of their workforce were neurodivergent. They had taken extensive measures to support these neurodiverse employees, including giving colleagues with autism ongoing training on how to manage relationships with line managers and hiring a welfare officer to assist with employee wellbeing. These initiatives were regarded as highly successful, and the firm felt that it was far more innovative as a result of its diverse workforce.

Barriers and challenges faced around diversity

One broad barrier to addressing the diversity issue was a lack of awareness, in several senses. For instance, whereas the gender diversity issue in cyber security appeared to be relatively well established, some interviewees had not previously considered the issue of neurodiversity.

In addition, diversity tended to be addressed at an organisation-wide level rather than within specific teams. Therefore, in organisations outside the cyber sector, the actions taken on diversity were often not specific to cyber security. In some cases, the cyber team heads in organisations outside the cyber sector

[24] Gender and ethnicity comparison data come from DCMS Sector Economic Estimates 2018: Employment (see https://www.gov.uk/government/statistics/dcms-sectors-economic-estimates-2018-employment).
[25] See https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund.

were not especially aware of the things their organisation was doing centrally on diversity or felt it was not their area of responsibility.

There was also a lack of awareness of general good practice. Some cyber team heads said they knew the issue was important but struggled to think of concrete actions they could take to improve the situation in their own organisation.

"I don't know what we can do really, apart from attracting more and more people to the positions."
Large organisation outside the cyber sector

"Gender is the one we struggle with and we would like to get more females in, but they just don't seem to be there, and I just haven't had the time to look at specifically targeting them. I wouldn't know where to start."
Cyber sector business

A specific issue raised around neurodiversity was with integrating neurodivergent employees into the workforce. There were examples where cyber firms had tried to employ neurodivergent individuals and found that they had different social norms to their colleagues, for instance around timeliness and attendance at meetings. There were also issues around the extent to which people would want to be open about any conditions they had. These organisations found there was a wider culture change needed when incorporating neurodivergent individuals into their workforce – something that could be supported by good practice guidance.

Diversity in recruitment processes

Our survey finds that 68 per cent of cyber firms have tried to recruit people in cyber roles in the last 3 years. Of these, relatively few say that they have adapted their recruitment processes or carried out any specific activities to encourage applications from diverse groups:

- 29 per cent have made changes to recruit more women
- 16 per cent have done so for ethnic minorities
- 16 per cent have done so for people with neurodiverse conditions or learning disorders

As might be expected, these proportions overlap. Among the cyber firms that have tried to recruit in the last 3 years, a total of 8 per cent report making changes to attract all 3 of these diverse groups.

However, 12 per cent of the firms that have tried to recruit say they have made changes to attract more women, but not done so with regards to ethnicity or neurodiversity. This highlights that there is typically more focus on gender than there is on other aspects of diversity.

Across the qualitative interviews, there was a sense of changes in recruitment practices being piecemeal and vague, as per the approach to diversity as a whole. However, there were some individual examples of good practice changes being made, including:

- Changing the wording of job adverts to be more inclusive
- Changing the minimum requirements for vacancies, removing specific qualifications or the need to have a degree, to allow a wider range of applicants

- One instance of a cyber firm working in partnership with a local charity, supporting young people, home carers and those on the autistic spectrum with training and work placement opportunities
- One case where a large business had worked in partnership with the National Autistic Society to overhaul all their recruitment processes to make them suitable for neurodiverse people

This suggests that recruitment is another area that could be supported by good practice guidance around diversity, laying out the concrete steps that organisations can take to improve their current recruitment practices.

4 Current skills and skills gaps

This chapter explores the cyber security skills that organisations say 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 in Chapter 6.

The wider context from external literature

- The DCMS Cyber Security Breaches Survey 2019 highlights that organisations may not be aware of their cyber security skills gaps. In this representative survey, three-quarters of UK businesses believe that the people dealing with cyber security in their organisation had the right cyber security skills and knowledge to do their job effectively[26]
- The 2018 Cybersecurity Workforce Study, which samples the views of very large global businesses, found that having relevant work experience and strong non-technical skills were considered more important than having a degree in cyber security or a related subject[27]
- The follow-up 2019 study highlights the following as areas where organisations want to improve their technical skills: cloud computing security; security engineering and administration; risk assessment; penetration testing; governance, regulation and compliance (GRC); intrusion detection; threat intelligence analysis; and network monitoring[28]
- The wider literature frequently highlights the importance of non-technical skills, including communication skills, teamworking ability and the ability to understand and harness wider disciplines such as law, business strategy and public policy. This includes a report from the Centre for Technology and Global Affairs[29] and the ISACA State of Cybersecurity 2019 report[30]

4.1 Awareness of the importance of different skillsets

The perceived importance of various technical skillsets outside the cyber sector

The quantitative survey asks organisations to rate the importance of different skills for those working in cyber roles. We split out basic technical skills, advanced technical skills and incident response skills. The definitions of basic and advanced in this context are spelled out in the survey, and are consistent with the DCMS definition of cyber security skills:

- Basic technical skills are the skills required to implement the 5 basic technical controls covered in the government-endorsed Cyber Essentials[31] guidance. These include: setting up firewalls, choosing secure settings for devices or software, controlling who has access, setting up antivirus protection and keeping software up to date. In the context of Cyber Essentials, these are the minimum skills that every organisation should possess to be cyber secure

[26] See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.
[27] See https://www.isc2.org/research.
[28] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study.
[29] See https://www.ctga.ox.ac.uk/article/beyond-awareness-breadth-and-depth-cyber-skills-demand.
[30] See https://cybersecurity.isaca.org/state-of-cybersecurity.
[31] 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. See: https://www.cyberessentials.ncsc.gov.uk/.

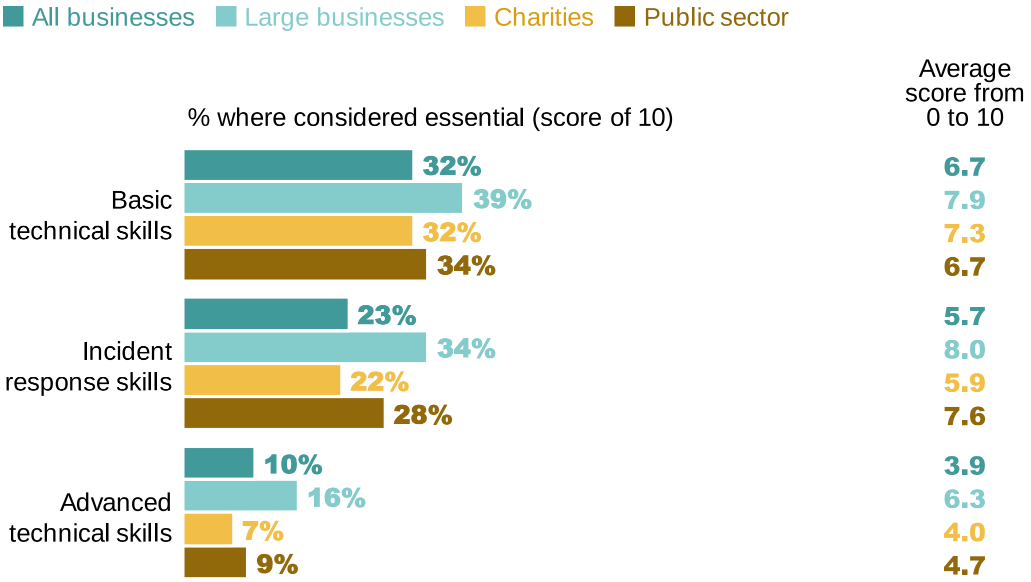
- The definition of advanced[32] technical skills came about through the extensive scoping research carried out as part of the 2018 labour market study. It includes any skills associated with security architecture or engineering, penetration testing, using threat intelligence tools, forensic analysis, 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

Figure 4.1 shows the results from the survey of general organisations (i.e. for cyber teams outside the cyber sector). A score of 0 means something is considered not at all important, while 10 means it is essential for cyber teams to have these skills.

Overall, these results highlight an overall lack of understanding of the importance of cyber security skills. Only around a third of organisations view basic technical skills – the skills that every organisation needs to implement minimal technical controls – as essential. This contrasts with the finding from the DCMS Cyber Security Breaches Survey 2019 that 78 per cent of all businesses and 95 per cent of large businesses consider cyber security to be a high priority.[26] It suggests organisations appreciate the importance of the issue but not necessarily the skills required to address it.

The findings also show that the vast majority of organisations outside the cyber sector do not feel they need advanced technical skills. The current demand for such skills is therefore likely to be concentrated among the largest organisations and the cyber sector.

Figure 4.1: Perceived importance of various technical skills areas for those working in cyber security roles outside the cyber sector



Bases: 1,046 businesses; 98 large businesses (with 250+ staff); 201 charities; 106 public sector organisations

In terms of sector differences, all 3 skill areas in Figure 4.1 are viewed as more important among organisations in the information and communications and health, social care or social work sectors. For example, 50 per cent of the organisations in each sector view basic skills as essential (vs. 32% overall).

A total of 4 in 10 businesses (40%) outsource at least some of their basic cyber security tasks to external cyber security providers. They may therefore not require basic skills in-house. However, when focusing

[32] In the survey questionnaire and in the 2018 study, we referred to these as “high level” technical skills.

on the 6 in 10 that perform all these basic functions internally, the results do not greatly differ, with 34 per cent saying basic skills are essential (vs. 32% overall) and an average score out of 10 of 7.0 (vs. 6.7 overall). This suggests a substantive gap in awareness of good practice and skills needs around cyber security, even among the organisations that do not get any outsourced help in this area.

The findings for basic and advanced skills are broadly unchanged from the 2018 survey. However, the proportion of businesses that view incident response skills as essential has increased by 6 percentage points this year, suggesting increased attention on this aspect of cyber security.

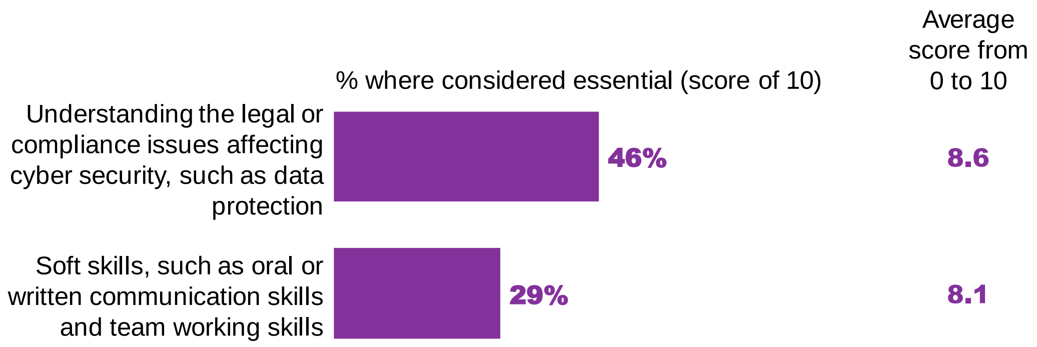
The perceived importance of non-technical skills within the cyber sector

For cyber firms, we assume that certain technical skills needs will be implicit based on the specialisation of the firm and also that each firm will have very bespoke technical skills needs (e.g. a firm specialising in penetration testing will not require network security skills to the same extent). Therefore, our survey focuses on the perceived importance of non-technical skills among these firms.

As Figure 4.2 shows, these firms tend to rate both a wider understanding of law and compliance and soft skills highly, as indicated by the high average scores out of 10. Nearly half (46%) consider it essential for their staff to have an understanding of legal or compliance issues and 3 in 10 see it as essential for them to have good soft skills.

It is worth noting that, across all UK businesses, there is likely to have been a renewed focus on legal and compliance issues in general in recent years, as a result of the General Data Protection Regulations (GDPR) which came into force in May 2018.

Figure 4.2: Perceived importance of various skills areas for those working in cyber security roles within cyber firms



Base: 205 cyber sector businesses

4.2 Technical skills gaps outside the cyber sector

Our approach to measuring skills gaps is consistent with the one used in the 2018 study. We ask organisations to tell us how confident they would be to carry out specific cyber security tasks or functions that require various skills. Those that are not confident are deemed to have a skills gap in this area.

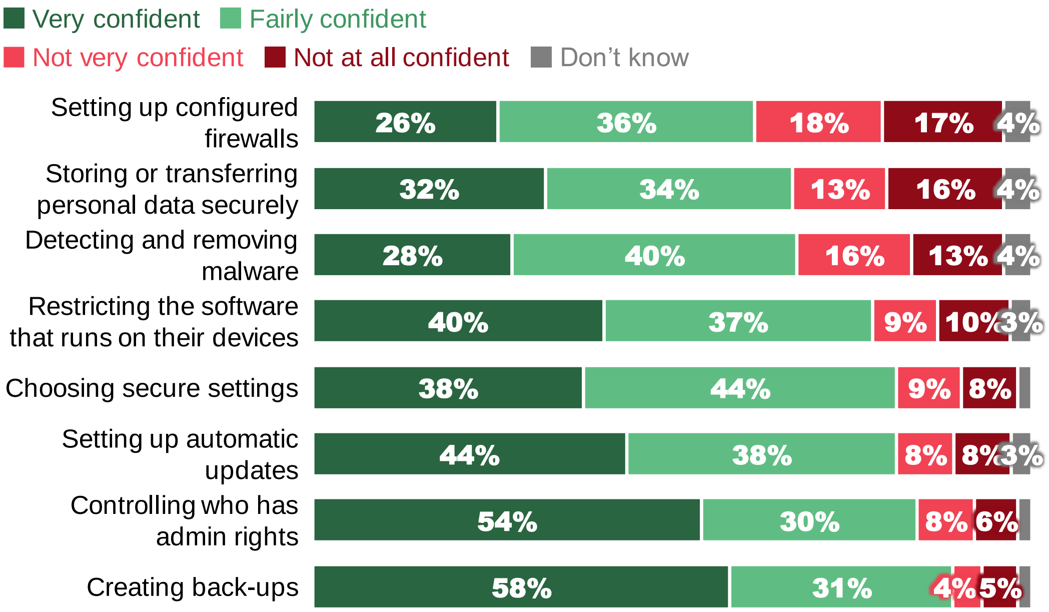
These questions each exclude organisations that say they outsource this particular cyber security task or function to external service providers, on the basis that those external providers fill the skills gap. We cover the proportions outsourcing each task in Chapter 8.

Basic technical skills

In the quantitative survey, the basic technical tasks and functions we ask about are a combination of the 5 technical areas covered under Cyber Essentials[31] (1 technical area, around secure settings for devices and software, is reflected in 2 statements) and 2 other aspects of cyber security highlighted by DCMS (securing data for storage and transfers and backing up data).

We focus initially on businesses. As Figure 4.3 shows, the 3 basic areas where skills gaps are most prevalent are in setting up configured firewalls, storing or transferring personal data, and detecting and removing malware. With that said, cyber leads in the majority of businesses that need to perform these tasks in-house are at least *fairly* confident at carrying out each of the 8 tasks.

Figure 4.3: Extent to which businesses are confident in performing basic cyber security tasks (where such tasks are not outsourced)

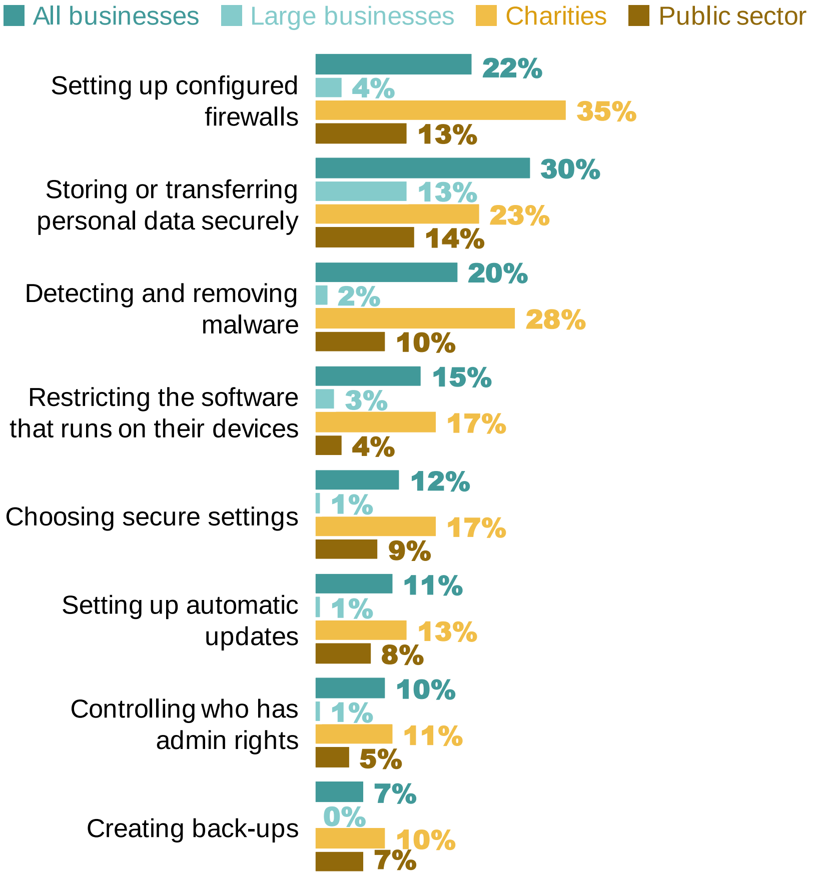


Bases: c.650+ businesses that do not outsource each task
Unlabelled bars are under 3%.

Figure 4.4 rebases the proportion that are not confident out of all businesses (i.e. including the businesses that outsource cyber security in the base) and compares this to charities and public sector organisations. The overall pattern is similar, although public sector organisations are, on the whole, less likely to have basic skills gaps than businesses or charities. Charities tend to have a greater skills gap than businesses when it comes to setting up configured firewalls.

Large businesses, also shown on the chart, are closer to public sector organisations in their reported ability to carry out these basic tasks in-house.

Figure 4.4: Percentage not confident in performing basic cyber security tasks, by type of organisation



Bases: 1,046 businesses; 98 large businesses (with 250+ staff); 201 charities; 106 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 are public sector organisations (c.50+).

Looking across business sectors, those in the information and communications, and finance and insurance sectors are among the least likely to identify basic skills gaps across all these tasks. This is expected – these are the sectors that tend to assign a higher priority to cyber security according to DCMS's Cyber Security Breaches Survey 2019.[26]

By contrast, basic technical skills gaps tend to be more prevalent among construction and retail and wholesale firms. All these sectoral differences are very similar to those found in the 2018 survey.

A combined basic technical skills gap indicator

To get an overall sense of the number of organisations that have any basic skills gap, we have combined the 8 tasks listed in Figure 4.3 and calculated the percentage of organisations that are not confident in carrying out 1 or more of these tasks.

By this measure, just less than half (48%) of all businesses have a basic technical cyber security skills gap. This is similar for charities (50%) and lower for public sector organisations (27%). As previously mentioned, the organisations that outsource these basic technical tasks and functions to external providers (see Chapter 8) are considered not to have a skills gap in these areas.

As this is a representative survey of the UK business population, we can extrapolate the 48 per cent result to indicate the total number of firms that have a basic technical skills gap. Of the c.1.36 million businesses in the UK, approximately 653,000 have a basic technical skills gap.[33]

This represents a 6-percentage point improvement for businesses compared with the 2018 survey (when 54% recorded a basic skills gap). This appears to be down to modest improvements across all the 8 basic skill areas in the survey, rather than a major improvement in a single area.

DCMS's Cyber Security Breaches Survey series found improvements in the proportion of businesses implementing the basic technical controls laid out in the Cyber Essentials guidance, between the 2018 and 2019 surveys. The 2019 report suggested that the introduction of GDPR had prompted businesses to act. The improvements in basic skills seen here may have a similar explanation.[26]

Knowledge of basic technical terms

The government-endorsed Cyber Essentials scheme also contains a basic checklist for organisations to follow.[34] 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.

- Only 40 per cent of those in charge of cyber security in the private sector and 43 per cent in charities say they understand the distinction between personal and boundary firewalls very or fairly well. This is slightly higher for public sector organisations (53%), although the findings indicate a common lack of understanding across all types of organisations

- Only a quarter each in the private or charitable sector (27% and 28% respectively) say they understand very or fairly well what a sandboxed application is. This is again higher among public sector organisations (57%)

There are no notable differences from the 2018 survey. As in 2018, these results highlight that, while a strong majority of organisations may 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 may slightly underestimate the true extent of the basic skills gap.

Advanced technical skills

Figure 4.5 shows how businesses fare at carrying out more advanced technical tasks and functions. These figures once again exclude those that say they outsource these particular areas and are therefore assumed to have no skills gap. In addition, we exclude those that say these skills areas are not important.[35] This recognises that not every organisation will require, for example, penetration testing. Therefore, in the context of this study, an advanced skills gap exists when an organisation:

- Identifies these advanced functions as an important part of their approach to cyber security
- Does not outsource them to an external cyber security provider

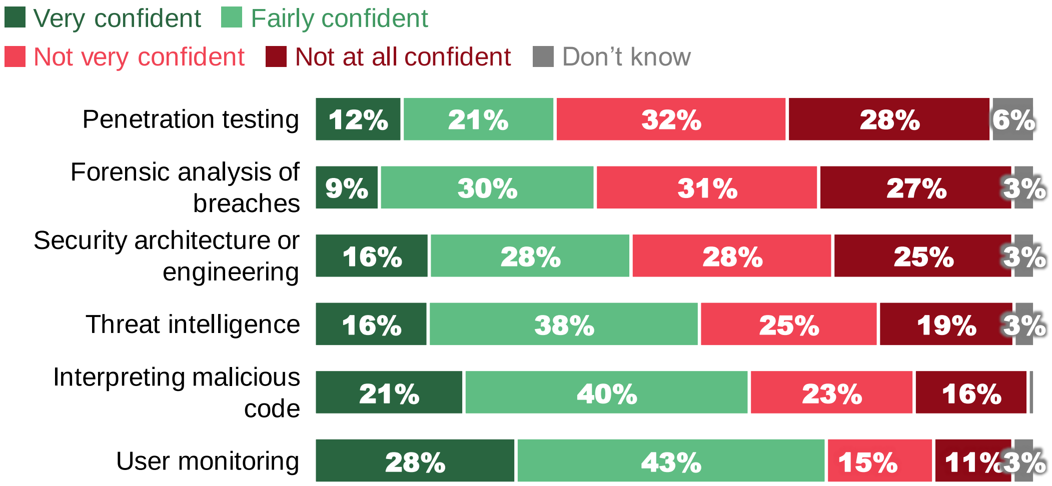
[33] The business population data is taken from the BEIS business population estimates in 2019. These are the latest estimates as of the publication of this report. See https://www.gov.uk/government/statistics/business-population-estimates-2019. For the extrapolated figures presented here and later in 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 ±4.1 percentage points. This means that the true figure could be between approximately 597,000 and 709,000 businesses. We have not made the same kind of extrapolation for charities or public sector organisations this year, given the relatively small sample sizes for these 2 groups.
[34] See https://www.cyberessentials.ncsc.gov.uk/advice/.
[35] This is defined as organisations giving a score of 0 to 4 (out of 10) for advanced technical skills at Figure 4.1.

- Is not confident at carrying out these functions in-house

To a small extent, this may underestimate the true skills gap in these more advanced technical areas. There may be firms that would benefit from carrying out activities such as penetration testing but have not invested in them. For this study, we have focused on skills gaps based on the cyber security skills that organisations *demand*, which may not match what they objectively *need*.

As Figure 4.5 illustrates, relative to what businesses demand, advanced skills gaps are most prevalent when it comes to penetration testing, forensic analysis and security architecture or engineering. These results are similar to the 2018 survey.

Figure 4.5: 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)

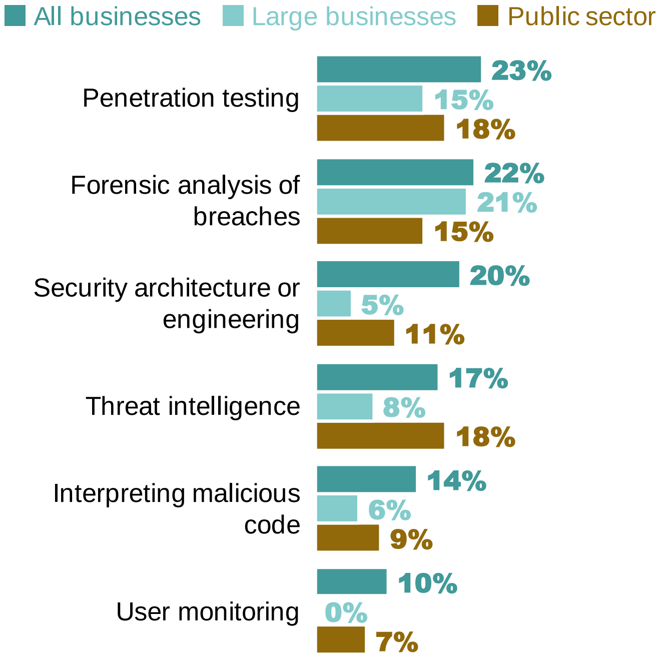


Bases: c.400+ businesses that do not outsource each task
Unlabelled bars are under 3%.

For Figure 4.6, we have rebased these findings out of all businesses (including those that either outsource these tasks or do not consider them as important). It shows that advanced skills gaps tend to be more prevalent in the private sector than in public sector organisations. There are too few charities sampled at this question to be reported here.

Once more, *large* businesses tend to have fewer skills gaps than the wider business population, but there are still more than 1 in 10 that have gaps in penetration testing and forensic analysis.

Figure 4.6: Percentage not confident in performing advanced cyber security tasks, by type of organisation



Bases: 1,046 businesses; 98 large businesses (with 250+ staff); 106 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 are public sector organisations (c.40+).

Extrapolating advanced technical skills gaps across the business population

We can once again extrapolate these figures to indicate the total number of private sector firms that have skills gaps in each of these more advanced technical areas of cyber security. For this analysis, we continue to use the rebased proportions from Figure 4.6. We find that:

- 313,000 businesses (23%) have a skills gap in penetration testing
- 299,000 businesses (22%) have a skills gap in forensic analysis
- 272,000 businesses (20%) have a skills gap in security architecture
- 231,000 businesses (17%) have a skills gap in threat intelligence
- 190,000 businesses (14%) have a skills gap in interpreting malicious code
- 136,000 businesses (10%) have a skills gap in user activity monitoring

A combined advanced technical skills gap indicator

As we do with basic skills, we have combined the 6 advanced cyber security tasks and functions from the previous section and calculated the percentage of organisations that are not confident in carrying out 1 or more of these tasks. This gives us a single figure for the advanced technical skills gap.

Once again, the organisations that outsource these advanced technical tasks and functions to external providers are, for the purpose of this study, considered not to have a skills gap in these areas. Those that do not think these kinds of advanced tasks and functions to be required for their organisation are also considered not to have an advanced skills gap.

A total of 3 in 10 businesses (30%) have an advanced technical skills gap, equating to approximately 408,000 UK businesses.[36] This is similar to charities (25%) and public sector organisations (27%).

4.3 Technical skills gaps within the cyber sector

The quantitative data in this section comes from a survey of the cyber sector carried out as part of the DCMS Cyber Sectoral Analysis 2020.[37] It is reported here for the first time. The survey methodologies used in both the sectoral analysis and this cyber security skills study are the same.

A total of 32 per cent of cyber firms say that existing employees lacking the technical skills they need has, at least to *some* extent, prevented them from meeting their business goals. In 5 per cent of cases, they feel this has prevented them to a *great* extent.

Similarly, 59 per cent of cyber firms say that job applicants lacking the technical skills they need has, at least to *some* extent, prevented them from meeting their business goals. Around a quarter (24%) feel this has prevented them to a *great* extent. This highlights that cyber firms see skills gaps as much more of an issue when it comes to recruitment, and less of an issue for existing staff.

Combining these results indicates that two-thirds (64%) of cyber firms have faced problems with cyber security skills gaps, either among existing staff or among job applicants. A quarter (25%) have faced more acute problems, saying that such skills gaps have prevented them to a great extent from achieving business goals.

Among this 64 per cent that have had any issues with skills gaps, Figure 4.7 shows which specific skillsets are considered lacking. The categories are based on the Chartered Institute of Information Security (CIISec, formerly IISP) Skills Framework.[38]

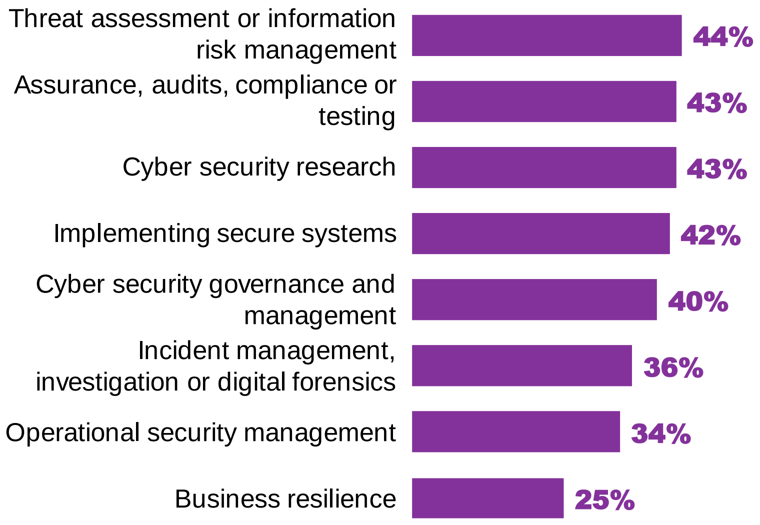
The results illustrate that there is no single technical area where skills gaps are more prevalent. Instead skills gaps are relatively high in each of the following areas: threat assessment or information risk management; assurance, audits, compliance or testing; cyber security research; implementing secure systems; and governance and management.

[36] Again, this extrapolated figure is subject to a margin of error. In this case, the margin of error is ±3.7 percentage points. This means that the true figure could be between approximately 358,000 and 458,000 businesses.

[37] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020.

[38] See https://www.ciisec.org/CIISEC/Resources/Skills_Framework.aspx. The latest version of the Skills Framework that was available during survey development was version 2.3.

Figure 4.7: Percentage of cyber firms that have skills gaps in the following technical areas, among those that have identified any skills gaps



Base: 169 cyber sector businesses identifying any skills gaps

4.4 Challenges and solutions when seeking specialist technical skills

Across the qualitative interviews, various areas were commonly mentioned as having more urgent skills gaps. These included penetration testing, forensic analysis, incident response and cloud security.

Larger organisations with heavy physical or digital infrastructure, such as energy companies or banks, also discussed an urgent lack of skills around industrial control systems and operational technology. This posed its own unique challenges, as some of these organisations were operating with legacy technology and required staff in cyber roles who were familiar with both old and new systems.

There was a sense that some technical areas were less elastic than others and therefore it was harder to transfer staff from other cyber security disciplines or teams to fill these skills gaps. For example, one cyber firm lead noted that penetration testing and forensic analysis teams could not easily be expanded with internal moves across teams because these areas required very specialised qualifications. They also mentioned that incident response teams could not easily be redeployed while they were on standby.

Interviewees highlighted that these kinds of highly specialised skillsets are in high demand and typically come with higher salary demands. This sometimes emerged as a more difficult challenge for public sector organisations, who were less able to compete on salaries with large private sector firms.

"Long gone are the days where you could have somebody with broad skills across cyber security. You absolutely must have deep technical skills."

Large organisation outside the cyber sector

Interviewees discussed various ways in which they had tried to tackle specialist skills gaps, including:

- More investment in training generally, including both internal training and sending staff on external courses to become accredited (discussed further in Chapter 5)
- More innovative knowledge sharing solutions, with job rotations and buddying used to transfer technical skills across teams
- Outsourcing to external cyber security providers to access bespoke skills as and when needed

- Identifying the skilled staff in cyber teams who would pose a risk to the organisation if they left
- In one case, looking abroad to recruit or outsource to people with specialist cyber security skills at a lower cost (in this case, in India)

One interviewee also highlighted the potential for more innovative solutions to fill specialist skills gaps. They suggested that there could be more technology based solutions, for example by automating aspects of penetration testing so that it reduced the burden on the human penetration testers. They also suggested that the government could issue a set of “grand challenges” to the cyber security industry to come up with more of their own innovative solutions to tackle skills gaps.

4.5 Future skills needs and challenges

The qualitative interviews also explored how cyber skills needs might change over the next 5 years. In these discussions, several technical skills areas were frequently mentioned, including cloud computing and storage, artificial intelligence (AI) and machine learning, threat intelligence, and skills to work with the Internet of Things. It is important to note that some of these areas, such as cloud computing, were also felt to be *current* skills gaps – the discussions about future skills needs simply reaffirmed perceptions that these skills gaps would become more acute over time.

Increasing the UK talent pool

While this study focuses on the current labour market, one of the main themes emerging from the qualitative interviews was the importance placed on addressing skills gaps through improvements to secondary and higher education. This included suggestions that pathways into cyber roles should begin in schools, with cyber security apprenticeships and degrees being promoted to students.

There was, for some, a perception that school teachers could know more about the breadth of cyber security careers, to give more effective careers advice to students. One interviewee noted that the current view of cyber security in schools was too focused on coding and that it could come across as a narrow subject area. Another mentioned that cyber security and computing generally could be better incorporated into the national curriculum.

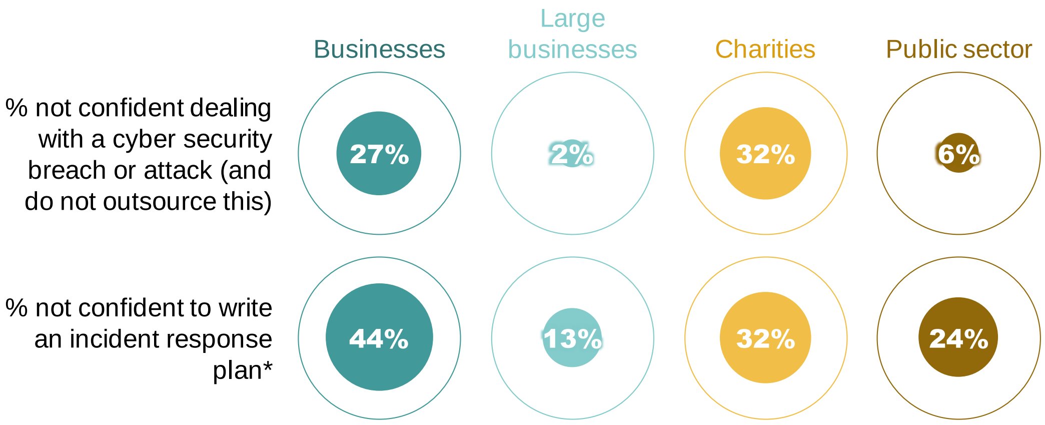
At the end of Chapter 6, we look at perceptions of the existing government schemes that aim to improve the pipeline of skilled individuals entering the cyber security labour market.

4.6 Incident response skills

Alongside technical skills gaps, incident response continues to be a challenging area for organisations. Just over a third of businesses (36%) outsource incident response. Among those that do not outsource it, 4 in 10 businesses (42%) are not confident that they would be able to deal with a cyber security breach or attack. This amounts to 27 per cent of all UK businesses (when including those who outsource it in the base).

As Figure 4.8 illustrates, over 4 in 10 businesses (44%) are also not confident in their ability to write an incident response plan.

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



Bases: 1,046 businesses; 98 large businesses (250+ staff); 201 charities; 106 public sector organisations
*Incident response plan question asked to random half of full sample (500 businesses, 47 large businesses, 92 charities, 54 public sector organisations).

We also ask cyber sector businesses about their confidence in writing an incident response plan. That is, a response plan for their own use, rather than for a client commissioning their services. As might be expected, a very low proportion (4%) say they would not be confident in writing such as plan.

As noted earlier in this chapter, the proportion of businesses that see incident response skills as essential has increased since the 2018 survey (from 17% to 23%). However, the findings discussed in this section have not changed, suggesting the incident response skills gap remains as large as before.

4.7 Soft skills

This section covers qualitative and quantitative findings on a range of soft skills, by which we mean things such as communication, client handling, consultancy, negotiation and the ability to manage and train others – all of which were mentioned in the qualitative interviews. Reflecting the wider literature as well as the 2018 study, we found soft skills to be an important feature for those working in cyber roles.

The importance and role of soft skills

In the qualitative interviews, those working in firms that provided cyber services to clients emphasised the importance of consultancy, client handling and communication skills for winning new work and maintaining good client relationships.

"Soft skills, like the ability to communicate well with client, are essential for us."
Cyber sector business

Cyber teams in large organisations also mentioned a need for cyber security staff who could sell cyber security messages upwards and downwards, to elicit behaviour change among wider staff. One cyber sector interviewee referred to these as cyber translators who could translate cyber risks into language that would engage businesspeople. They felt these skills would become increasingly important as cyberattacks and cyber security become more sophisticated.

"We need someone with the ability to collaborate with senior stakeholders and technical people."
Cyber sector business

A common theme was that it was challenging to find someone with the right technical skills *and* good soft skills of this kind. For example, one interviewee mentioned that senior staff were often recruited for their technical proficiency and experience, but this did not guarantee that they were good leaders or people managers. Some felt, therefore, that it was important for existing external training courses in cyber security to incorporate soft skills.

Do cyber sector firms identify a soft skills gap?

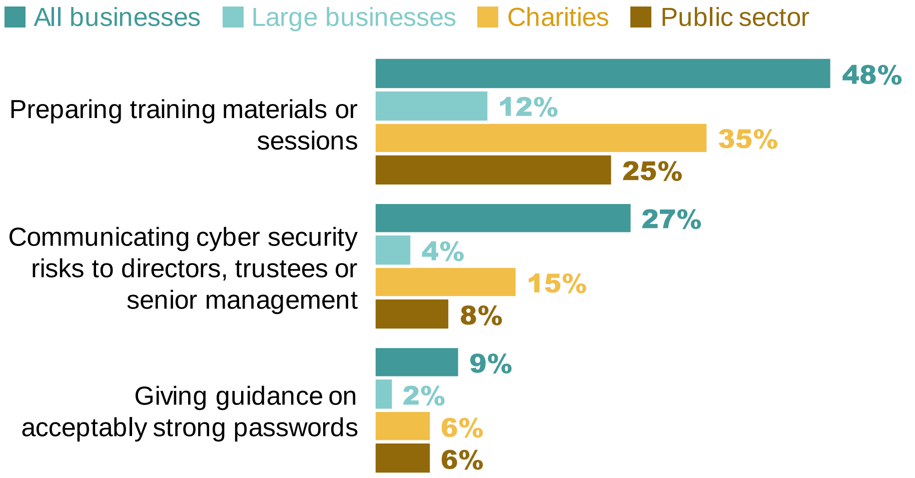
The following quantitative results come from the cyber sector survey carried out as part of the DCMS Cyber Sectoral Analysis 2020 (which used the same methodology as our survey for this study).[37] They are reported here for the first time.

- A total of 3 in 10 cyber firms (29%) say that job applicants lacking non-technical skills such as communication, leadership or management skills has prevented them from meeting their business goals. In 9 per cent of cases, they report that this has prevented them to a *great* extent.
- Similarly, 3 in 10 cyber firms (28%) say that existing employees lacking these non-technical skills has, at least to *some* extent, stopped them from meeting their business goals. In 5 per cent of cases, they say this has been to a *great* extent.

Comparing these to the results on technical skills in Section 4.3 suggests that a lack of technical skills and soft skills are equally prevalent issues when it comes to job applicants in the cyber sector.

Our survey for this study also covers soft skills gaps, focusing on specific activities such as communicating risks, communicating good practice and developing training. These tasks require a mix of technical knowledge and soft skills to be carried out effectively. The results in Figure 4.9 suggest that there are significant gaps in communication and in preparing training for those currently in cyber roles in the private sector.

Figure 4.9: Percentage <u>not</u> confident in carrying out a range of tasks that require soft skills



Bases (asked to a random half of full sample): c.500 businesses; c.50 large businesses (250+ staff); c.90 charities; c.50 public sector organisations

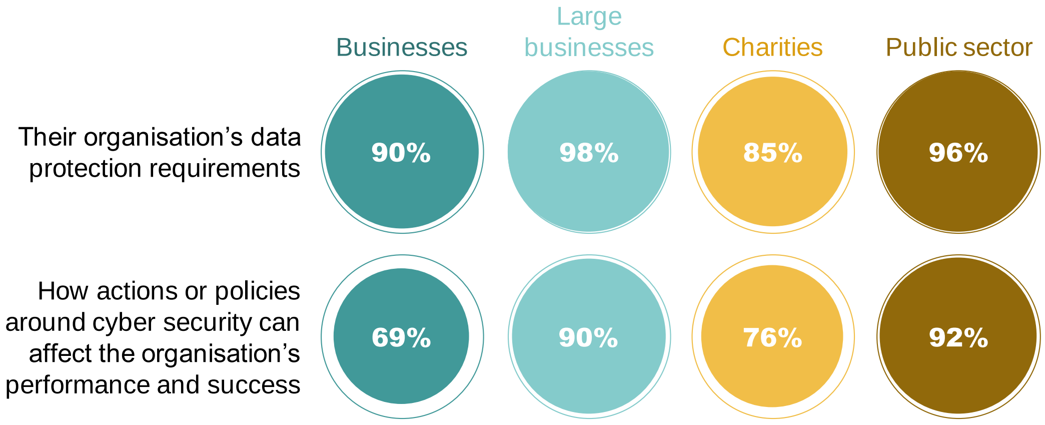
4.8 Strategic management and planning ability

The 2018 labour market study established that those in senior cyber roles need strategic management skills to perform their role effectively, particularly the governance, regulation and compliance (GRC) aspects. This includes being able to understand and work to rules and regulations. It also involves understanding of how cyber security can best fit within a business context, with minimal disruption.

As Figure 4.10 demonstrates, a majority of organisations do not consider themselves to have knowledge gaps in this area. However, a sizeable minority of cyber leads in the private sector admit to being uncertain about how cyber security can affect business performance (29% not very or at all well).

These findings are consistent with those reported in 2018.

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

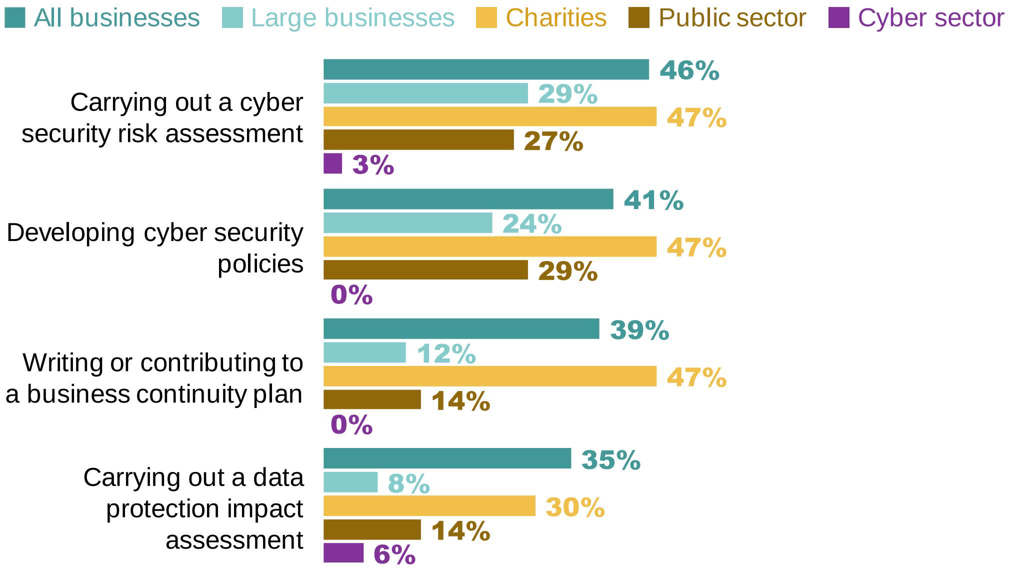


Bases (asked to a random half of full sample): c.500 businesses; c.50 large businesses (250+ staff); c.90 charities; c.50 public sector organisations

Nevertheless, the self-reported understanding in Figure 4.10 is not matched by high levels of confidence in carrying out typical cyber security governance tasks. As Figure 4.11 suggests, 4 in 10 private sector cyber leads are not confident in their ability to develop cyber security policies or write a business continuity plan. There are also similar skills gaps evident in carrying out cyber security risk assessments and data protection impact assessments.

Cyber sector businesses are overwhelmingly confident at being able to carry out these tasks for their own organisation. Cyber leads in public sector organisations are also typically more confident than those in private sector firms.

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.500 businesses; c.50 large businesses (250+ staff); c.90 charities; c.50 public sector organisations; c.100 cyber sector businesses

4.9 The increasing need for a holistic skillset

In the qualitative interviews, a major recurring theme was around the importance of staff in cyber roles having a combination of different types of skills rather than focusing on individual gaps in skills and knowledge. This issue was raised from several different angles:

- Across several interviews, the importance of implementation skills – being able to implement technical knowledge in a business context – was frequently raised
- Knowledge of multiple technical areas was especially important for staff working in managed service providers, given that they needed to be able to talk credibly with clients on multiple topics
- One cyber team head said that it was rare to find staff that had both technical skills and a wider understanding of GRC concepts
- Another interviewee highlighted that the number of products and tools in cyber security had grown. Therefore, cyber firms were often looking for people with multiple accreditations, as well as a willingness and ability to learn new tools quickly

"Finding people who have the broad brush approach and a holistic understanding of cyber security is challenging. Cyber security can mean a lot of different things for different clients."
Cyber sector business

"Looking back 10 years, an organisation might have 5 or 6 security products that they needed to run within the business. Now you're into 20, 30 or even 50 different tools."
Cyber sector business

4.10 Cyber security skills gaps in the non-cyber workforce

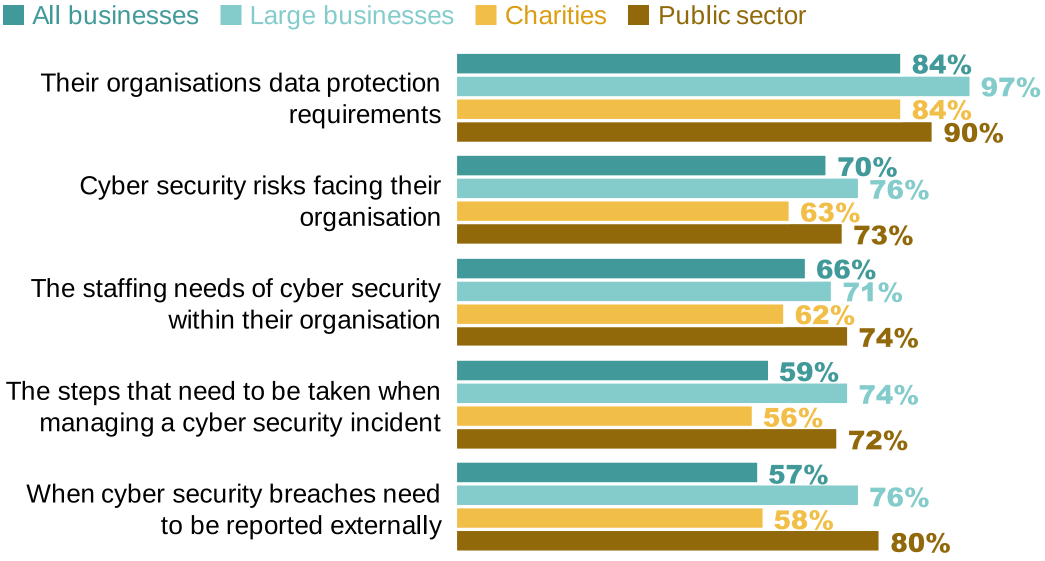
In the 2018 survey, we identified that senior managers and wider staff outside of cyber teams also needed to have the right skills and knowledge to be able to understand and interpret cyber risks, recognise their GRC responsibilities, and follow the cyber security rules and processes set by their organisation. This section explores skills and knowledge gaps among 2 groups.

Cyber security skills at the board level

Figure 4.12 highlights the scepticism among a quarter or more cyber team heads in private sector businesses when asked to rate senior managers' understanding of cyber security. 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.

There is a sense that senior managers have a relatively better understanding of their organisation's data protection requirements, compared to the other areas reported here. Again, this result should be seen in the context of GDPR, which has renewed the focus on data protection in management boards.

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: 1,046 businesses; 98 large businesses (with 250+ staff); 201 charities; 106 public sector organisations

Cyber team heads in finance and insurance businesses tend to be more positive about the cyber security skills of their senior boards. For example, 89 per cent say their senior managers understand when breaches need to be reported externally (vs. 59% overall). By contrast, cyber leads in construction firms and transport and storage firms often tend to be less positive their senior managers' understanding.

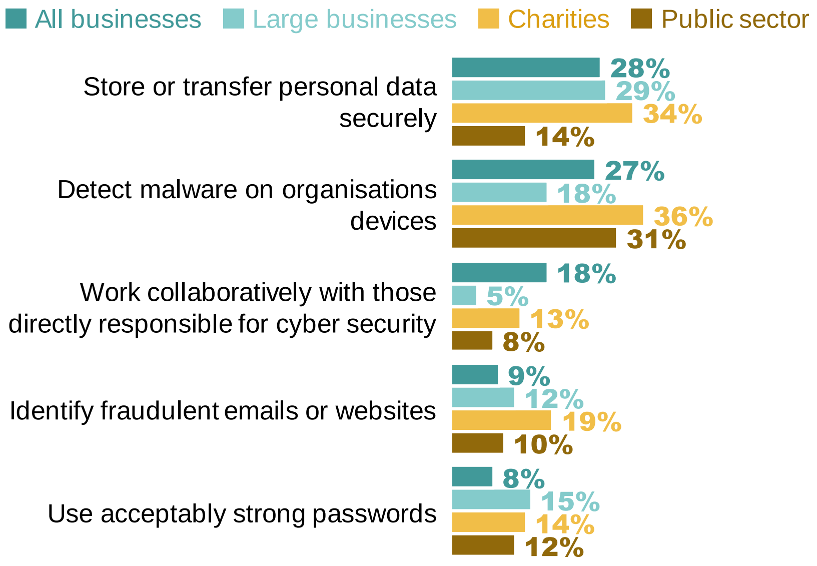
While these findings suggest an ongoing lack of understanding of cyber security on the part some of management boards, there are signs of improvement compared to the 2018 survey. Across 3 areas, the proportion of cyber leads reporting that senior managers understand these areas well has increased:

- The cyber security risks facing their organisation (from 62% in 2018 to 70% now)
- Their cyber security staffing needs (from 59% to 66%)
- The steps required to manage a breach (from 52% to 59%)

Cyber security skills among wider staff

When it comes to wider staff (i.e. those outside of cyber teams), cyber leads across different types of organisations are, on balance, confident that they can carry out various tasks without posing a risk to cyber security. The full list of tasks is shown in Figure 4.13, and show that the greatest concerns relate to staff being able to store and transfer personal data securely and to detect malware on their devices.

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



Bases: 1,046 businesses; 98 large businesses (with 250+ staff); 201 charities; 106 public sector organisations

Across each of these indicators, cyber team heads in the information and communications sector tend to be more confident than average about their wider staff acting appropriately when it comes to cyber security. For example, 90 per cent are confident that their wider staff can store and transfer personal data securely (vs. 66% overall).

Broadly, these results are in line with the 2018 survey. However, even though this remains an area of concern, more private sector cyber leads are now confident in the ability of wider staff to store and transfer personal data correctly (up from 58% in 2018 to 66% now).

5 Training and upskilling

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

Unique to this chapter, we also draw on findings from the qualitative interviews we carried out with 7 cyber security training providers as part of the scoping stage for this study.

The wider context from external literature

- The Enterprise Security Group and the Information Systems Security Association (ISSA) survey of global ISSA members has consistently found that organisations need to hire and train more junior staff as a result of cyber security skills shortages[39]
- Similarly, InfoSecurity Magazine's qualitative research with 60 global cyber security leads finds that more investment in training for junior cyber security staff is one of the key areas that organisations could improve on[40]

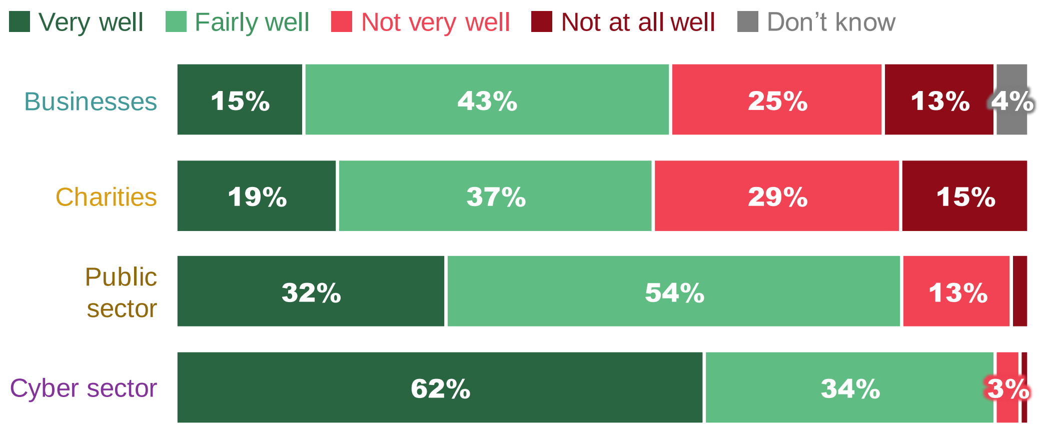
5.1 Training needs

How well organisations feel they understand their training needs

Most organisations feel they understand their cyber security training needs well (very or fairly), but few outside the cyber sector say they understand them *very* well, as Figure 5.1 shows. This proportion is higher among public sector organisations than private sector ones (32% vs. 16%).

In the case of cyber sector businesses, 6 in 10 (62%) do feel they understand their training needs very well. However, this still leaves 4 in 10 that do not pick this top answer, suggesting room for improvement.

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



Bases: 1,046 businesses; 201 charities; 106 public sector organisations; 205 cyber sector businesses
Unlabelled bars are under 3%.

[39] See https://www.esg-global.com/esg-issa-research-report-2018.
[40] See https://www.infosecurity-magazine.com/white-papers/state-of-cybersecurity-report-2019-1/.

Looking at different business sectors, finance and insurance businesses, and information and communications businesses are more likely than average to say they understand their training needs very well (28% in each case, vs. 16% overall). Construction firms are, by contrast, most likely to say not at all well (21%, vs 13% overall).

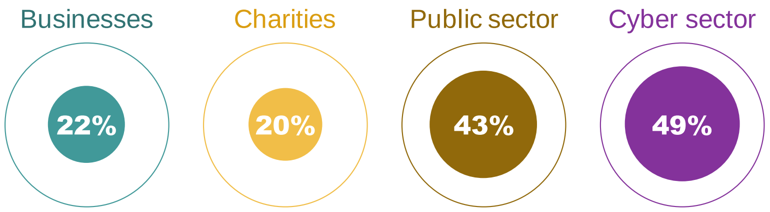
Large businesses also tend to have a better sense of understanding of their training needs, with a quarter saying they understand them very well (26%, vs. 16% overall) and 6 in 10 saying they understand them fairly well (60%, vs. 43% overall).

Formally analysing training needs

The self-reported understanding of training needs can be contrasted against the proportion that have undertaken formal training needs analyses. As Figure 5.2 shows, just 2 in 10 businesses (22%) and charities (20%) have done this in the past year.

For businesses, this proportion is higher than in 2018 (up 6 percentage points from 16%) – although, as covered later in this chapter, this is not matched by a similar increase in actual training undertaken.

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



Bases: 1,046 businesses; 201 charities; 106 public sector organisations; 205 cyber sector businesses

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

- Finance and insurance (55%, vs. 22% overall)
- Health, social care and social work (34%)
- Information and communications (32%)
- Education (31%)

The challenge for newcomers navigating the cyber security training market

In the qualitative research with training providers, there was broad agreement that it was difficult for individuals starting out in the industry to know how different training aligned to different cyber roles, and that potential training routes and qualifications could be incorporated into documented career pathways or roles frameworks.

"I think there's massive confusion out there. How is someone new supposed to know, 'where do I start?' There are some war stories out there, with cyber courses being badly managed by providers, or not reflecting the variety of cyber roles out there."
Cyber security training provider

Providers also highlighted the importance of having training courses that were more geared towards new entrants without previous experience in cyber roles. This includes courses and programmes that:

- Focus on the basics, for example short modules on networking or security principles
- Incorporate soft skills as well as technical elements
- Establish training cohorts, so that people leave with a sense of community and a wider network
- Are linked to employment outcomes

Another recurring theme was around making training more accessible to diverse groups looking to enter the profession, such as women returning from maternity leave, those with military backgrounds and neurodiverse groups. For instance, there was a perception that current training courses are too skewed towards London, making it harder for those who have to travel to reach them.

One provider noted that, in the context of people moving from military to cyber roles, it was important for training schemes to show how different cyber roles potentially aligned to military ones, to help people from this background to navigate the market.

"You can take a veteran and say: 'you worked well within a military operations centre in Afghanistan, so that's not far removed from a SOC Analyst role.'"
Cyber security training provider

Another provider raised the ongoing need to educate employers about alternative training approaches, noting that exam based training courses are often not suited to people with neurodiverse conditions.

"With the Cyber Security Skills Immediate Impact Fund (CSIIF), it has been more about educating the employers, that despite potentially being previously unemployed or without relevant qualifications, this person can offer a lot to your business."
Cyber security training provider

5.2 Training undertaken by those in cyber roles

A total of 1 in 4 businesses (24%) report having any of their staff in cyber roles undertake training in the last year. This is in line with the 2018 result.

This proportion is similar for charities (29%). It is considerably higher among public sector organisations (66%) and, as might be expected, cyber sector businesses (73%). However, this still suggests that 1 in 4 cyber firms have not carried out any staff training in the past year.

As a broad baseline, this might be compared to the Employer Skills Survey, which produces biennial statistics on training across all businesses. The latest data, from the 2017 survey (published in 2018, Department for Education) shows that 55 per cent of employers have provided job specific training to any of their staff over a 12-month period. This statistic has remained unchanged for several years.[41] Relative to this, the incidence of training in the public and cyber sectors compares favourably, but this is not the case for the private and charitable sectors.

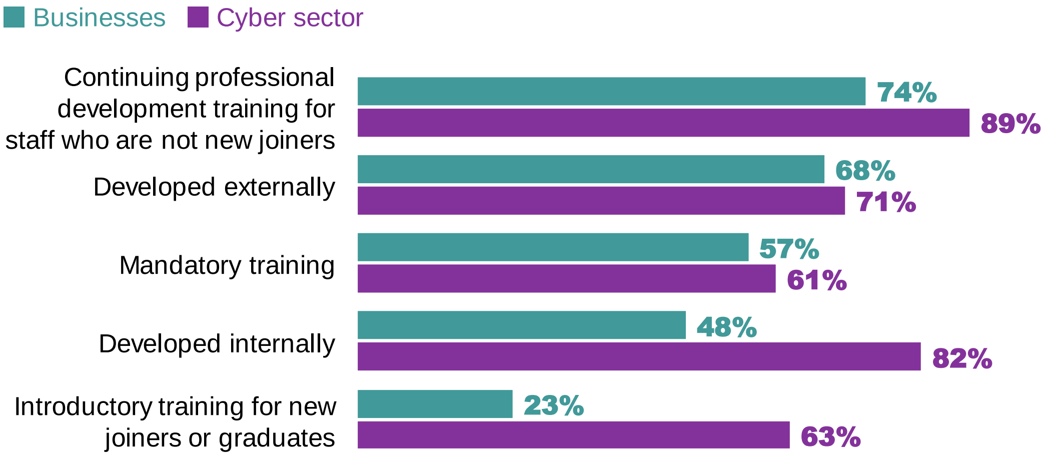
Figure 5.3 shows the nature of this training, among the firms that provide it. We show findings for all businesses and for cyber firms, but the pattern of findings is similar for charities and public sector

[41] See https://www.gov.uk/government/publications/employer-skills-survey-2017-uk-report.

organisations. It highlights that training is more commonly directed at established cyber staff rather than new joiners or graduates.

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. For example, 54 per cent of the cyber sector organisations that provide training have used *both* externally and internally developed 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: 254 businesses that have had staff in cyber roles undertake training; 150 cyber sector businesses that have had staff in cyber roles undertake training

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

- Finance and insurance (56%, vs. 24% overall)
- Education (41%)
- Information and communications (46%)
- Health, social care and social work (40%)

It is also far more likely for medium (57%) and large businesses (59%) to provide such training than the average business.

5.3 Cyber security training or awareness raising activities for wider staff

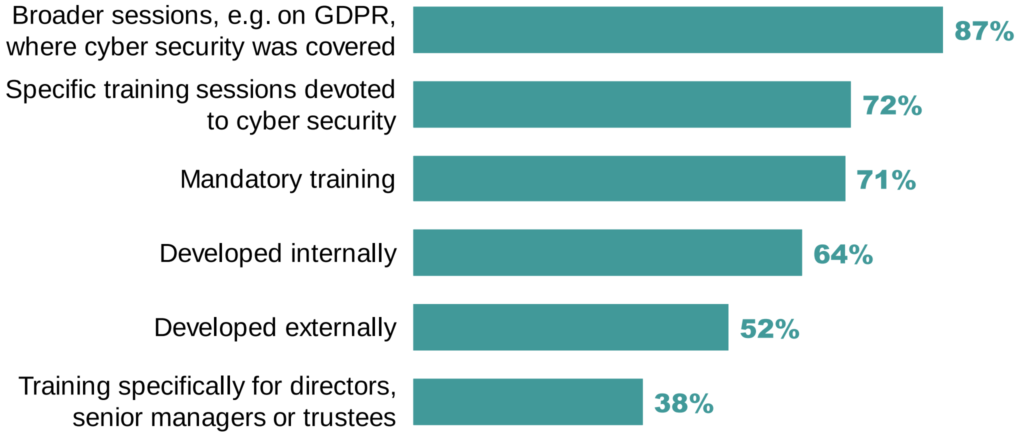
Overall, 1 in 9 businesses (11%) have provided cyber security training to non-cyber employees in the last year. There are substantive differences by size, with this kind of training being much more common in medium (32%) and large businesses (47%). Public sector organisations are also much closer to large businesses in this regard, with around half (54%) having provided this kind of training.

As Figure 5.4 shows, these training sessions are not always focused exclusively on cyber security, and they often incorporate other aspects like the General Data Protection Regulations (GDPR). The training is typically mandatory, but in 3 in 10 cases (30%) in the private sector, it is not.

This wider staff training is more likely to be internally developed than externally developed. Only in half of cases (48%) do businesses offer external training.

Training designed for management boards is relatively rare, accounting for just 39 per cent of the cases where businesses are providing cyber security training to any non-specialist staff. This equates to just 4 per cent of all businesses.

Figure 5.4: 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: 231 businesses that have undertaken training or awareness raising sessions for non-specialist staff

Cyber security training for wider staff is much more prevalent in the finance and insurance sector than any other (44%, vs. 11% overall). It is also more likely to be found in the information and communications sector (28%). By contrast, this kind of training is especially rare among construction businesses (3%).

Interpretation of the trend data (and a comparison to the Cyber Security Breaches Survey series)

The DCMS Cyber Security Breaches Survey series has a different question that tracks the prevalence of cyber security training each year. Between the 2018 and 2019 surveys, it found that the proportion of businesses where any staff members (in cyber roles or otherwise) had attended any kind of cyber security training, seminars or conferences in the previous 12 months had risen (from 20% to 27%).[42] The 2018 and 2019 surveys were carried out before and after the introduction of GDPR respectively, linking this increase to GDPR.

By contrast, our 2018 skills survey and this latest survey both took place after GDPR came into being in May 2018. Across these surveys, we do not observe any change in the proportion of businesses providing cyber security training to non-specialist staff. Therefore, the impact of GDPR on cyber security training may have already peaked – the businesses that would have instigated training because of GDPR appear to have already done so.

5.4 Effectiveness of training

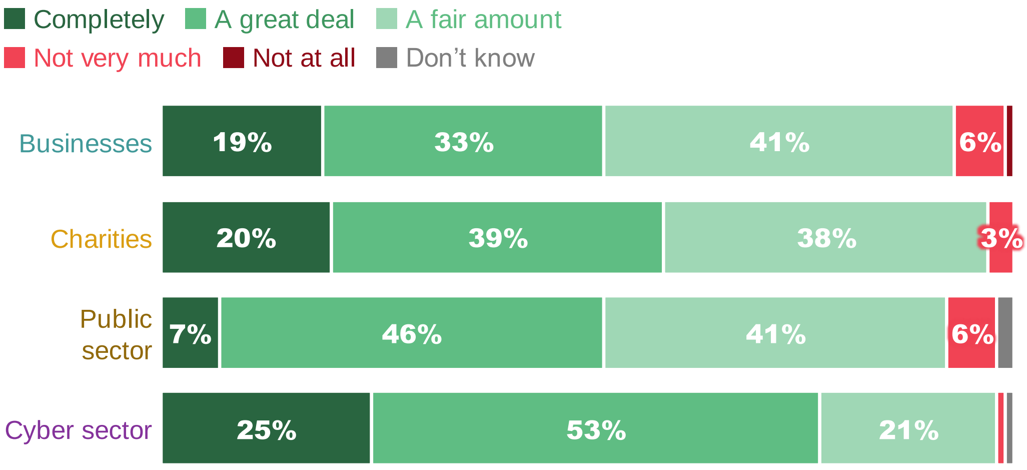
Training for those in cyber roles

Figure 5.5 shows that the organisations that have invested in training for those in cyber roles are, on balance, positive about the effectiveness of this training. However, outside the cyber sector, around 4 in 10 organisations feel the training only met their needs *a fair amount*.

[42] See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.

For businesses outside the cyber sector, these results are consistent with those recorded in 2018.

Figure 5.5: 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): 387 businesses; 85 charities; 70 public sector organisations; 150 cyber sector businesses
Unlabelled bars are under 3%.

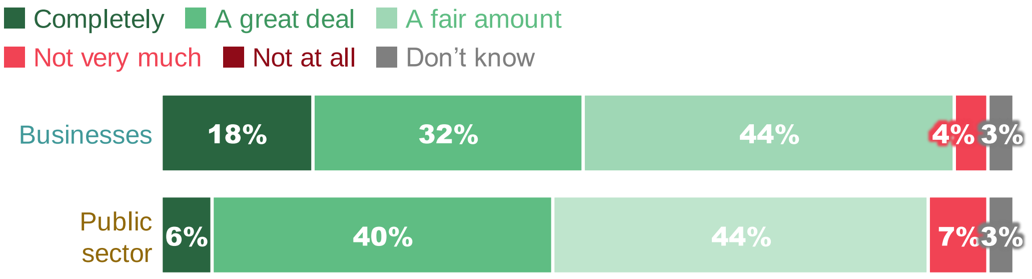
Reflecting on the wider findings in this chapter, there could be a range of explanations for the results in Figure 5.5. For instance, it could be that firms outside the cyber sector have a harder time trying to navigate the training provider market to find appropriate training. It could also be related to the earlier finding that these organisations are less certain of their training needs than those in the cyber sector.

Training for wider staff

When it comes to the perceived effectiveness of cyber security training for wider staff, the pattern of responses is very similar to those in the previous section. That is, most are positive on balance, but a large proportion (44% of businesses) think that training only met staff needs *a fair amount*.

We report results for businesses and public sector organisations. There are too few charities providing training in our sample to report results for this group. Cyber firms are not asked this question.

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



Bases (among organisations that have undertaken training or awareness raising sessions for non-specialist staff): 387 businesses; 70 public sector organisations

What do cyber team heads think makes training more effective?

In the qualitative interviews (both with training providers and with the organisations requesting training), there were some common themes around effective training approaches:

- In several instances, cyber team heads discussed the importance of training not coming across as boring or as hard work. They felt that training needed to be visually engaging and interactive, for example by giving trainees mini tests to pass after each segment of online training. Gamification was also mentioned. For example, one business had set up a competition across teams for completing online courses. Another was planning to have more cyber incident role-playing sessions to test how people would implement their incident response skills

- Training providers highlighted that training formats needed to be varied for the best outcomes. Some stressed that bootcamp style training or 9 to 5 courses could exclude those already with full time jobs. It was, in their view, important to have a mix of approaches that allowed people to learn at their own pace, for example with online labs and sessions. At the same time, face to face contact was still often viewed as the best way to get people to complete their training

- Many cyber team heads highlighted the importance of internal on-the-job training. As was often noted, this enabled employees to develop and apply their cyber security knowledge in a specific business context, as well as learning the internal standards and processes they have to work within. On-the-job training was also felt to circumvent some of the challenges associated with formal classroom or web based training, such as the cost, or courses being too theoretical

> ***"There aren't a lot of qualifications out there that are more business focused on the cyber aspects."***
>
> *Cyber sector business*

- One cyber team head detailed the main factors that they looked for when choosing online cyber security training packages for non-specialist staff. The first was around integration – how well it could be incorporated into their wider programme of training overseen by their human resources team. Flexibility was important, in terms of quickly and easily adding new modules to respond to new threats. Finally, they wanted good reporting tools that could easily identify who had completed training modules and the specific areas that staff had performed less well on

5.5 Barriers and challenges around training

The qualitative interviews with large organisations and cyber sector businesses raised a host of challenges around training. There were also a range of suggestions for how the government might help with some of these challenges.

- Training was perceived to be costly, both financially and in terms of the time commitment from staff. One cyber team head suggested that more flexible and broader apprenticeship frameworks and standards (previously discussed in Chapter 2) could help alleviate the financial burden by enabling them to fund a wider range of apprentices in cyber roles. Another suggested potentially having a centralised training budget for cyber firms to tap into. Some also highlighted the National Cyber Security Centre's (NCSC) free e-learning packages for wider staff as a positive step

- The constant evolution of cyber security – in terms of a changing threat landscape, the introduction of new technologies, products and vendors, and changing client needs – was raised as a challenge. It meant that cyber leads needed to stay on top of developments in the training market and that training needs analyses had to be regularly updated. In particular, cyber firms that worked with multiple cyber security products needed to spend time researching the large number of vendor-specific accredited training courses. As part of this, some organisations had set up a skills matrix or register to keep track of all the different skills and accreditations that their cyber staff had

- There was a sense that the quality of vendor-specific accredited training could vary greatly. This had led some organisations to choose training providers based mostly on word of mouth feedback from industry peers. One cyber firm had alternatively asked vendors to carry out office visits to their firm in cases where the online training had not received good feedback. Here, there was a suggestion that the NCSC was already considered a credible voice and could help endorse or rate training providers to help raise quality standards

- There was a common perception that current training products could be too theoretical and not business orientated enough. As we noted in Chapter 2, qualifications were not seen to guarantee that someone was able to effectively apply their knowledge in a business context. A related concern was that training courses often did not focus enough on soft skills

- The multiplicity and practicality of skills frameworks was sometimes an issue. Cyber leads mentioned a wide range of frameworks across interviews, including the Cyber Security Body of Knowledge (CyBOK)[43], the Chartered Institute of Information Security (CIISec, formerly IISP) Skills Framework[44], the National Initiative for Cybersecurity Education (NICE) framework[45] and the Skills Framework for the Information Age (SFIA)[46]. There were mixed thoughts on their usefulness, as they did not map to accreditations or qualifications. One cyber lead mentioned that it might be helpful for the NCSC to recommend a specific framework, such as CyBOK, for organisations to use or adapt

[43] See https://www.cybok.org/.

[44] See https://www.ciisec.org/CIISEC/Resources/Skills_Framework.aspx.

[45] See https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/current.

[46] See https://www.sfia-online.org/en/framework.

6 Recruitment and retention

This chapter deals with organisations' approaches to recruitment and retention, 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. We also cover awareness and perceptions of current government initiatives aiming to increase the number of job ready applicants.

The 2020 quantitative survey findings on this topic are exclusively for cyber sector businesses. In the 2018 survey, we found that just 2 per cent of all private sector businesses had carried out external recruitment for anyone for a cyber role in the preceding 3 years. The low incidence reflected that cyber sector businesses are the high volume recruiters in this labour market, hence the decision to focus on these businesses this year.

The qualitative data is broader and covers both the cyber firms as well as the large organisations outside the cyber sector that we interviewed. As such, a large part of this chapter covers the qualitative findings.

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. This was a more experimental methodology, so we have opted to give it its own chapter (Chapter 7).

The wider context from external literature

- Cyber security skills shortages are a global issue. Two-thirds of the (mainly large) global businesses sampled in the 2019 ISC2 Cybersecurity Workforce Study have a cyber security skills shortage.[47] EY's Global Information Security Survey 2018-19 similarly finds that skills shortages are on a par with budgets as a constraint on cyber security[48]
- A report by the Enterprise Security Group and the Information Systems Security Association (ISSA), based on a survey of global ISSA members, found that the cyber security labour market tends to be a seller's market, with three-quarters of respondents being chased by external recruiters at least once a month[49]
- InfoSecurity Magazine's qualitative research with 60 global cyber security leads suggests the need for more realistic hiring processes that do not expect new hires to be immediately deployable and have a comprehensive technical background. It instead suggests more entry-level hires accompanied by greater investment in training by firms[50]

6.1 Approaches to recruitment and retention

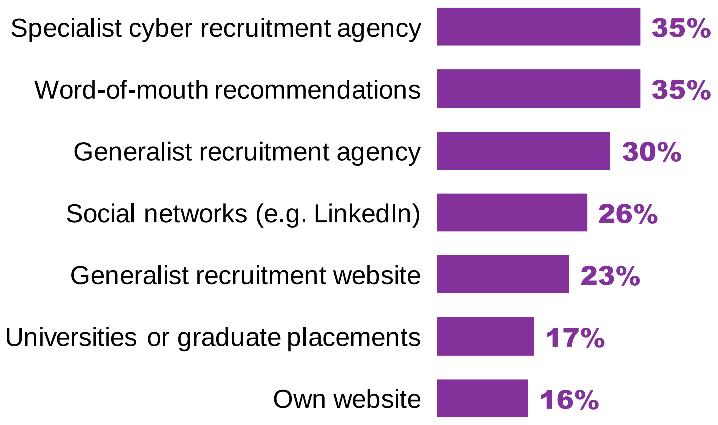
Most common recruitment methods

Around 7 in 10 cyber sector businesses (68%) have tried to recruit someone in a cyber role within the last 3 years. The unprompted list of the most common recruitment methods used to find candidates for these roles is in Figure 6.1. It suggests that the use of recruitment agencies, social networks and offline networking (with industry peers or at events and conferences) is especially common.

[47] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study.
[48] See https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf.
[49] See https://www.esg-global.com/esg-issa-research-report-2018.
[50] See https://www.infosecurity-magazine.com/white-papers/state-of-cybersecurity-report-2019-1/.

By contrast, there is relatively little use of print adverts (4%) and direct applications (through company websites or just asking people to apply – also 4%). It is also relatively rare for recruitment to be aimed at graduates – a theme we return to across this chapter.

Figure 6.1: Percentage of cyber firms with vacancies in the last 3 years that have used the following recruitment methods (unprompted)



Base: 139 cyber sector businesses that have had vacancies in cyber roles in the last 3 years
Only specific categories mentioned by 10% or more shown.

Current recruitment approaches are not particularly diverse. A quarter (27%) 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 (33%) have used 2 methods and just under two-fifths (37%) have used 3 or more methods.

In the qualitative interviews, more diverse recruitment methods tended to be clustered among the largest cyber sector businesses. They often used a mix of apprenticeship schemes, placements, careers fairs, graduate schemes and headhunting. This suggests an imbalance between larger and smaller firms, with the former having more resources to dedicate towards recruitment – particularly for career starters.

Recruiting foreign nationals

It is commonplace for UK cyber firms to try to fill skills shortages by recruiting foreign nationals. Around 4 in 10 (41%) cyber firms say they could *completely* meet their skills needs by recruiting staff from the UK residential labour market rather than elsewhere. However, 54 per cent do not believe that recruiting UK staff alone could meet their needs. For 1 in 10 (10%) this problem is more acute – they say their skills needs would be met hardly at all or not at all if restricted to recruiting UK staff.[51]

6.2 Hard-to-fill vacancies and skills shortages

Among the 68 per cent of cyber sector businesses that have had any cyber security vacancies in the past 3 years, more than half (57%) had at least 1 vacancy that they considered to be hard to fill. Looked at another way, this equates to around a third (35%) of all the vacancies posted in the last 3 years being hard-to-fill vacancies. This gives an indication of the size of the cyber security skills shortage.

Reasons behind hard-to-fill vacancies

As Figure 6.2 shows, among the cyber sector businesses 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

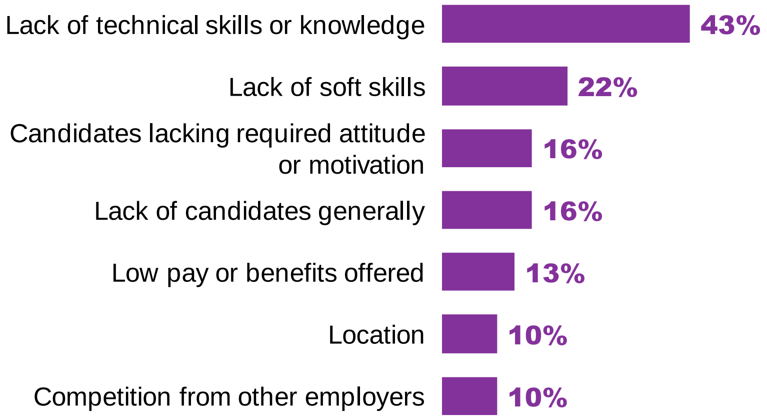
[51] These findings come from the separate cyber sector survey carried out as part of the DCMS Cyber Sectoral Analysis 2020. The findings are reported here, where they are most relevant, rather than in the sectoral analysis report. Both studies have a matching survey methodology.

knowledge. This once again highlights that relevant technical skills are the single most important element that employers are looking for when recruiting for cyber roles.

Nevertheless, it is worth noting that this is not the reason given in more than half of cases. Instead, businesses commonly highlight other issues contributing to their skills shortage, including applicants lacking soft skills or the right attitude. This reflects the desire for applicants to have a more holistic skills mix, which we discussed in Chapter 3.

A quarter (27%) of these businesses admit that their employment offer is not competitive enough. We discuss the challenges around salaries and competition with other employers in the next section.

Figure 6.2: Most common unprompted reasons offered by cyber sector businesses for having hard-to-fill vacancies



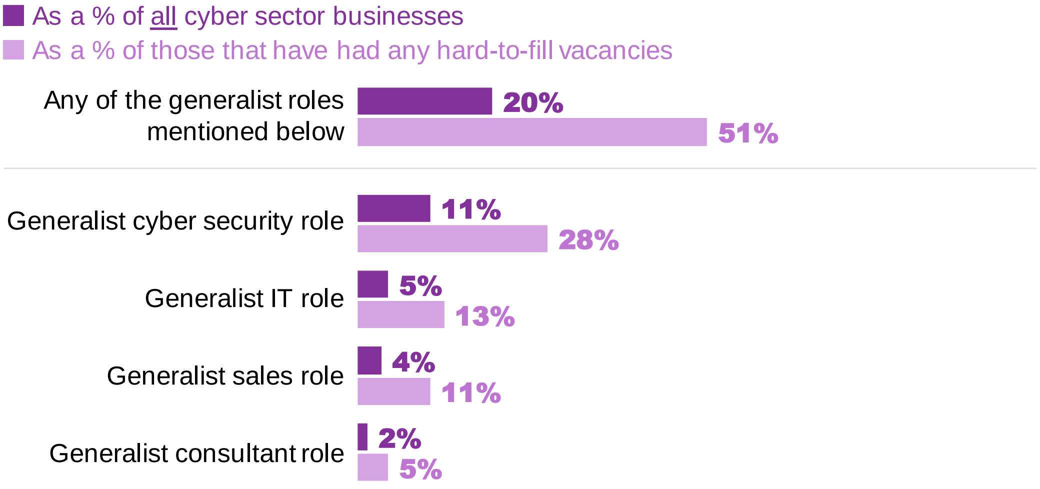
Base: 79 cyber sector businesses that have had hard-to-fill vacancies in cyber roles in the last 3 years
Only specific categories mentioned by 10% or more shown.

Specific roles most affected by skills shortages

The survey findings suggest that there is an even mix of skills shortages across both generalist and specialist cyber roles. In this context, generalist roles are ones 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, half (51%) say they have had such vacancies in generalist roles. This amounts to 20 per cent of all cyber sector businesses. It includes positions that are formally labelled as cyber roles, as well as IT, sales or consultancy roles that require cyber security knowledge or involve cyber security functions – broken down in Figure 6.3.

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

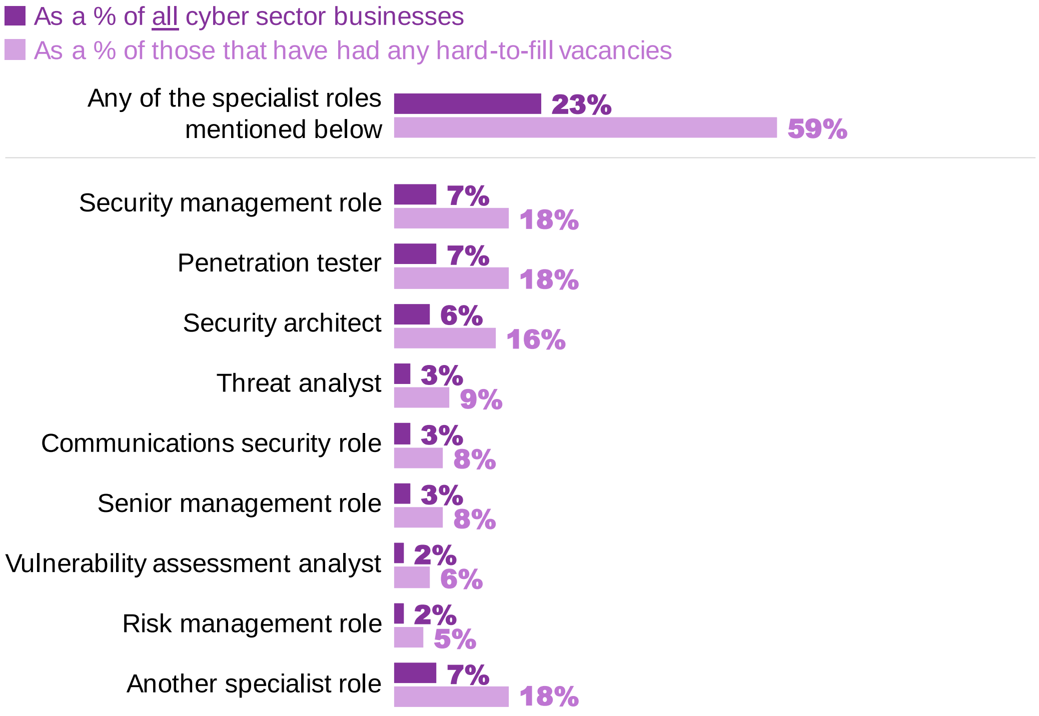


Bases: 205 cyber sector businesses; 79 that have had hard-to-fill vacancies in cyber roles in the last 3 years

Among those that have had hard-to-fill vacancies, 6 in 10 (59%) have had such vacancies in specialist roles. This equates to 23 per cent of all cyber sector businesses.

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.[52] This framework covers 8 specialist cyber roles. The most common skills shortages are in security management, penetration testing and security architecture.

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



Bases: 205 cyber sector businesses; 79 that have had hard-to-fill vacancies in cyber roles in the last 3 years

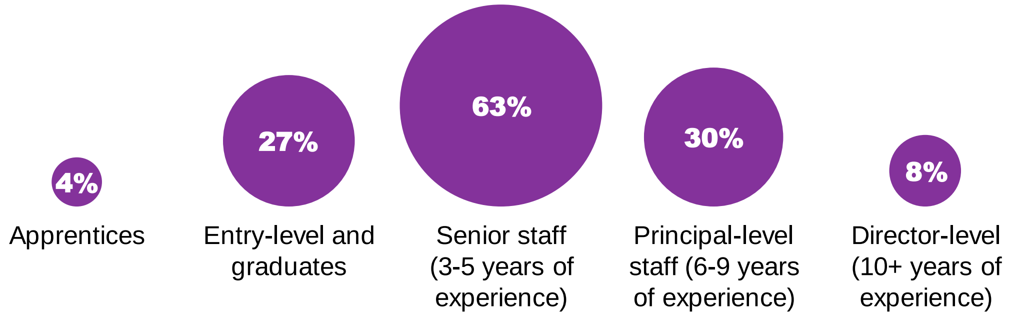
[52] See https://www.ciisec.org/CIISEC/Resources/Roles_Framework.aspx. In the survey, respondents are given a fuller description of each role if they require it.

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).

There seems to be less of a skills shortage at entry level roles. However, this may reflect that relatively few cyber firms are aiming to recruit people at this level. The data on pathways into cyber security covered in Chapter 2 and the job vacancy data in Chapter 7 both suggest this.

Figure 6.5: Percentage of cyber sector businesses that have found it hard to fill positions at the following levels, among those that have had hard-to-fill vacancies



Base: 79 cyber sector businesses that have had hard-to-fill vacancies in cyber roles in the last 3 years

6.3 Staff turnover

Staff turnover is another challenge for cyber firms. A total of 4 in 10 cyber firms (40%) expect at least 1 member of staff in a cyber role to leave within the next 12 months. Among this group, the average firm expects to see 3 out of every 10 staff members leave (31% of all their staff) over the coming year.

The vast majority (74%) of this group of firms are confident that they will replace the skills lost when these staff leave. However, a quarter (23%) are not confident.[53]

6.4 Main challenges faced in recruitment and retention

This section focuses on the common issues around recruitment and retention emerging from the qualitative research.

Challenges around having a competitive employment offer

Salaries were commonly raised as a challenge across all types of organisations, within and outside the cyber sector. There was a sense that some job applicants set their salary demands too high and were unwilling to work at the rates that businesses could afford.

Some organisations noted that wage differentials by sector and between London and the rest of the UK exacerbated this gap. There were mentions of large IT companies and those in the finance sector being able to outbid other sectors. For example, one interviewee highlighted that someone in an analyst role in a finance firm in London could potentially earn over £80,000 within 2 years of graduating from university – much higher than it was possible for them to offer when based outside London. The issue of inflexible pay structures in the public sector also came up, with one public sector interviewee saying this stopped their organisation from offering the market rate.

[53] These findings come from the separate cyber sector survey carried out as part of the DCMS Cyber Sectoral Analysis 2020. The findings are reported here, where they are most relevant, rather than in the sectoral analysis report. Both studies have a matching survey methodology.

"It becomes a bidding war. We are outbid by offers of higher salaries elsewhere."

Cyber sector business

Another broader issue raised was the inherent attractiveness of cyber security work in sectors. For example, one cyber team head for a large business noted that their business sector might be less appealing to someone than a role in a defence firm.

"Ours is not the most interesting industry. People want to move on to companies who are doing all the flashy stuff."

Large organisation outside the cyber sector

Where organisations were not able to compete on salaries alone, many looked to improve the non-financial benefits they offered to staff. This included:

- Flexible and remote working policies, especially for organisations outside London
- Improving training, acknowledging that paid-for accredited training was a highly attractive benefit
- Giving staff mapped and transparent career pathways

Job applicants misrepresenting their abilities

One issue, which was linked to inflated salary demands, was the sense that people were frequently applying for roles that they did not have the skills or experience to perform. Some interviewees felt that applicants had recognised that there was a small talent pool for specialist cyber roles and were prone to exaggerating their expertise and experience in CVs. This was then picked up at the interview stage, at a cost to employers.

"I got the perception that people were trying their luck, jumping on the cyber security bandwagon with little experience and demanding a good salary, which wasn't warranted."

Large organisation outside the cyber sector

Mismatches between job roles, frameworks and accreditations

The 2018 labour market study established that smaller organisations outside the cyber sector faced an additional problem in recruitment – their lack of in-house knowledge of cyber security meant they often did not know what skills they should be looking for in job applicants.

By contrast, this year's qualitative interviews focused on very large organisations and firms in the cyber sector. These organisations typically reported having a very good idea of the specific skills they needed, and how to describe these in job adverts. However, the difficulty of aligning job descriptions to specific qualifications was raised. This reflected both the plethora of qualifications and accreditations in the market, and the perception that qualifications were often not good indicators of implementation skills.

"It is difficult to define requirements, so I have basically given up. I don't mention any technologies in particular in my job descriptions."

Cyber sector business

Organisations had used a variety of frameworks, such as the Cyber Security Body of Knowledge (CyBOK)[54], CIISec Roles Framework and the US National Initiative for Cybersecurity Education (NICE)

[54] See https://www.cybok.org/.

framework[55], to help them write job descriptions. The latter framework and the organisation behind it, the National Institute for Standards and Technology (NIST) were more commonly mentioned in this regard.

However, there were suggestions that the available roles frameworks could be improved. For example, one interviewee felt that the NICE framework was overlong and impractical to use in recruitment. Another interviewee noted that the CIISec Roles Framework was more aligned to government roles than to commercial roles. They also felt that roles frameworks did not map well to qualifications, which also made it difficult to align job descriptions to specific qualifications.

Problems with recruitment agencies

Improving the effectiveness of recruitment agencies was a common theme. The heads of cyber teams often thought that recruitment agencies that did not specialise in cyber security did not understand the market well. This included a perceived lack of understanding of the multitude of industry qualifications and accreditations, and the different roles in cyber security. It was also felt that agencies did not distinguish between candidates that simply understood technical concepts versus those that could practically implement these concepts or carry out consultancy work.

These issues were felt to have increased applications from unsuitable candidates. This had driven some cyber team heads towards greater use of personal networks in recruitment. They felt that applicants recommended through word of mouth were more likely to have the kinds of skills that recruitment agencies might overlook, and which would not be apparent solely from people’s qualifications and accreditations, such as their implementation skills and communication skills.

> ***“If you need a specific skill, you’ve got to know people with that skill, or know people who know people. That’s the only thing that really works.”***
> *Large organisation outside the cyber sector*

Some cyber sector businesses had started using specialist cyber security recruitment agencies, which they felt produced better matches. However, changing recruiters was often harder for organisations outside the cyber sector. Some were tied to centralised recruitment agencies, arranged through their human resources department and used for multiple cyber and non-cyber business roles. There was a significant time investment for organisations to find specialist recruiters and establish good relationships with them. Specialist recruiters were also reported to be more expensive.

6.5 How organisations are addressing the challenges

Openness to more innovative approaches

Across the qualitative interviews, there was an appetite for broader, as well as more innovative approaches to help overcome skills shortages. There were several examples of this, notably a greater focus on career starters, partnerships, work placements and diversifying the pool of applicants:

- Various organisations had moved more towards recruiting and upskilling career starters such as apprentices and graduates. One interviewee felt that this had led to job applicants with fewer preconceptions about working in cyber security and a strong willingness to learn

[55] See https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center/current.

- In one case, a large cyber firm had scrapped their previous minimum requirement for job applicants to have a 2.1 degree. Instead, they now focused more on people's cyber and non-cyber backgrounds, their problem solving abilities and their other relevant accreditations

- There were instances of organisations offering flexible working or post-maternity return to work schemes to encourage a wider group of people to apply, including more women. However, it was still rare for organisations to see workforce diversity as a way of addressing skills shortages

- There were several examples of work placements. As first discussed in Chapter 3, one cyber sector business was working with a local charity to offer work placements to people with neurodiverse conditions.[56] Another cyber team head was aware of a recruitment agency that was running a programme offering extended work placements in cyber security, of around 2 to 3 months, to those coming from military roles – they were keen on this approach but had not used this agency due to the high fees

> ***"The first school pupil we took on, he came for a week and we sat him alongside one of our junior developers … We encourage them to come back to us. And they came back for 2 weeks. And we got them to fly on their own."***
>
> *Cyber sector business*

Internal recruitment

The qualitative research specifically explored internal recruitment as a way of addressing skills shortages in cyber roles. Interviewees felt this way of recruiting often had advantages. This included being able to recruit people who had already bought into an organisation's ethos. Some felt it made it easier to find people with the right mindset or attributes not necessarily captured in qualifications and accreditations, such as a sense of inquisitiveness. It has also been a way for some organisations to build technically skilled cyber teams without having to pay unaffordable salary premiums.

"Internal recruitment enabled us to grow our own talent and not have to compete on the open market, where the wages were much higher."

Large organisation outside the cyber sector

Internal recruitment was felt to be more successful when staff who were already in technical roles (e.g. IT roles) or had technical backgrounds (e.g. in scientific occupations) moved into cyber roles. Where this was not the case, some organisations had struggled to bring internally recruited individuals up to speed. Some were also concerned that the on-the-job training and mentoring needs of new recruits placed, or would place, a burden on other team members.

Bad experiences with one recruitment approach had often led organisations to pivot. In these cases, some organisations, especially those with small cyber teams, had ruled out any future internal recruitment based on their negative experiences to date.

[56] Neurodiverse conditions or learning disorders include autism, Asperger syndrome, dyslexia, dyspraxia and attention deficit hyperactivity disorder (ADHD). We cover workforce neurodiversity in more detail in Chapter 3.

6.6 Perceptions of government initiatives

In the qualitative interviews, we probed awareness and perceptions of 3 government initiatives, which are intended to tackle current skills shortages in cyber security and improve the pipeline of skilled individuals in the future:

- The Cyber Skills Immediate Impact Fund (CSIIF), which provides government funding for training programmes targeting groups that are currently underrepresented in the cyber sector[57]
- CyberFirst, which covers a range of activities and programmes aimed at young people aged 11 to 19, including bursary and cyber apprenticeship schemes, a girls-only competition and school development courses at UK universities and colleges[58]
- Cyber Discovery, an online extracurricular training programme for young people aged 13 to 18[59]

While many interviewees had at least heard of the schemes, there was a sense that awareness and knowledge of these schemes was not as widespread as it should be, particularly within the cyber sector. Some wanted to see more marketing to cyber firms and management boards, explaining how they could take advantage of initiatives like the CSIIF.

Those we spoke with often did not have much detailed knowledge of these schemes. Therefore, the feedback we received is relatively broad and was based on perceptions rather than people's first hand experiences. With that said, there was generally a positive reception to these initiatives. However, those that had heard of them felt the government could increase investment and run programmes on a larger scale. It was a common perception that the government had a significant role to play in increasing the talent pool, particularly by helping to attract more young people into cyber security careers.

The importance of long term funding was also mentioned. One interviewee suggested that schemes like these should be funded for 5 year cycles, so that the labour market could better adapt to them, knowing that they would not disband after a year.

There were also suggestions that schemes like CyberFirst and Cyber Discovery could be better targeted. Some felt that they were skewed towards young people with an existing interest in cyber security or who had more parental support, which might continue to exclude more diverse groups. One interviewee felt that CyberFirst could also give a broader view of the kinds of non-technical skills required in various cyber security roles, such as good governance and communication.

Finally, there was a sense that the entire programme of government activity on cyber security skills could be more joined up. This meant knowing how different initiatives relate to one another and how they fit into a broader career pathway from school to employment.

[57] See https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund.
[58] See https://www.ncsc.gov.uk/cyberfirst/overview.
[59] See https://www.joincyberdiscovery.com/.

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.

As this is a relatively experimental methodology, there are no comparisons drawn here against the wider literature on cyber security skills.

7.1 Core versus cyber-enabled job roles

The separately published technical report comprehensively lays out the methodology used for this analysis.[60] An important aspect to bear in mind when reading this chapter is that 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 <u>both</u> 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 many organisations (typically micro ones) 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.

[60] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020.

7.2 Number of job postings

The broad search results yield a total of 393,257 cyber security-related job postings in the UK between the start of September 2016 and the end of August 2019 (a 3-year period). This includes:

- 105,194 core cyber job postings
- 288,063 cyber-enabled job postings

These figures should not be considered as a definitive stance on the number of jobs in cyber security in the UK. Instead, they are our best estimate of the number of job postings that contain tasks, responsibilities or skillsets well aligned to the cyber security discipline.

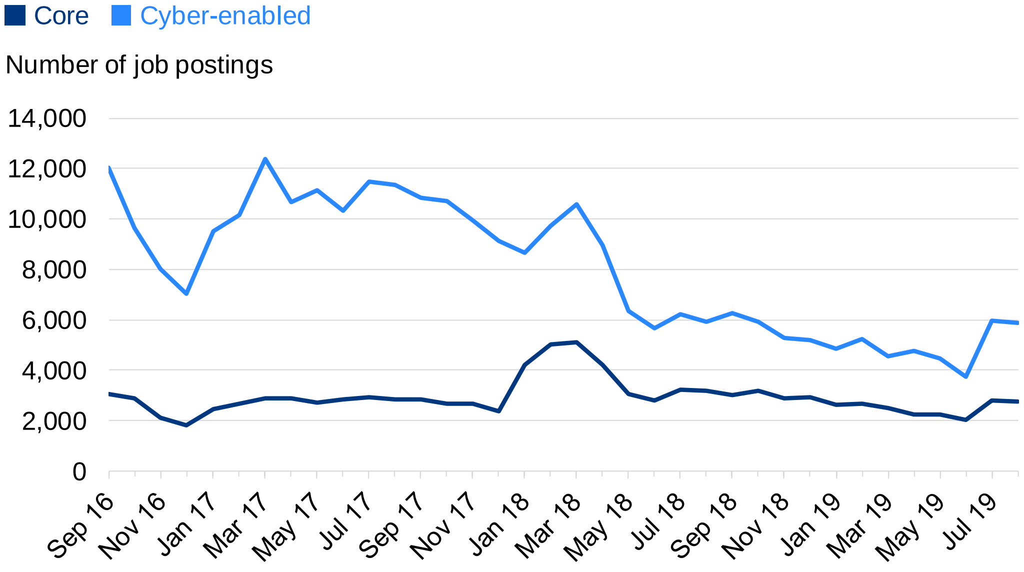
Changes over time

Across the three-year period, on average there have typically been approximately 11,000 job postings each month, of which c.3,000 per month have been core cyber roles. The demand for people in these core cyber roles has been much more stable than the demand for the wider array of cyber-enabled jobs.

The monthly breakdown of job postings in Figure 7.1 demonstrates that demand for cyber talent was particularly high in the 6-month period (November 2017 to May 2018) prior to the introduction of the General Data Protection Regulation (GDPR). It has subsequently reduced to a level that has been relatively sustained post-May 2018.

There may be other factors linked to the volatility of monthly job postings, and the apparent decline in cyber-enabled job postings since late 2016. For example, some employers may have initially used external recruitment to build an internal cyber security team and then moved towards other closed forms of recruitment not captured in these statistics (e.g. headhunting or referrals) as their cyber security needs have become more sophisticated, or in response to growing skills gaps.

Figure 7.1: Monthly number of core and cyber-enabled job postings from September 2016 to August 2019



Source: Burning Glass Technologies

Benchmarking against other cyber security employment estimates

There have been existing attempts to understand the size and scale of the cyber security workforce in the UK, and to understand gaps in supply:

- DCMS's Cyber Sectoral Analysis 2020 estimates 42,855 full time employees working in cyber roles in the UK cyber sector, across the 1,221 cyber security companies that make up this sector.[61] However, this excludes individuals working in cyber roles outside of these companies

- Also, recently, the 2019 ISC2 Cybersecurity Workforce Study report has estimated that there are c.289,000 people in the UK cyber security workforce.[62] By our analysis, this is an underestimate of the size of the workforce. Their report does not explain which roles are included or excluded, and this may in part be the source of the difference

- In 2017, the Tech Partnership estimated that there were c.58,000 people working in cyber security in the UK. They also estimated that there were c.7,000 vacancies per month in 2017, and that this figure had increased by 18 per cent between 2016 and 2017[63]

Within our analysis, we have identified 393,257 job postings over 3 years, of which 105,194 can be considered core cyber roles. This means that there are approximately 35,000 core and 95,000 cyber-enabled roles in scope each year, which is broadly consistent with the Tech Partnership's estimate of 7,000 vacancies per month (and its respective increase of c.18% per year).

7.3 Geographic differences

Figure 7.2 shows the proportion of job postings for core cyber roles from each UK region (where the region is known). Given the large amount of source data, these are shown to 1 decimal place to highlight the small differences between certain regions.

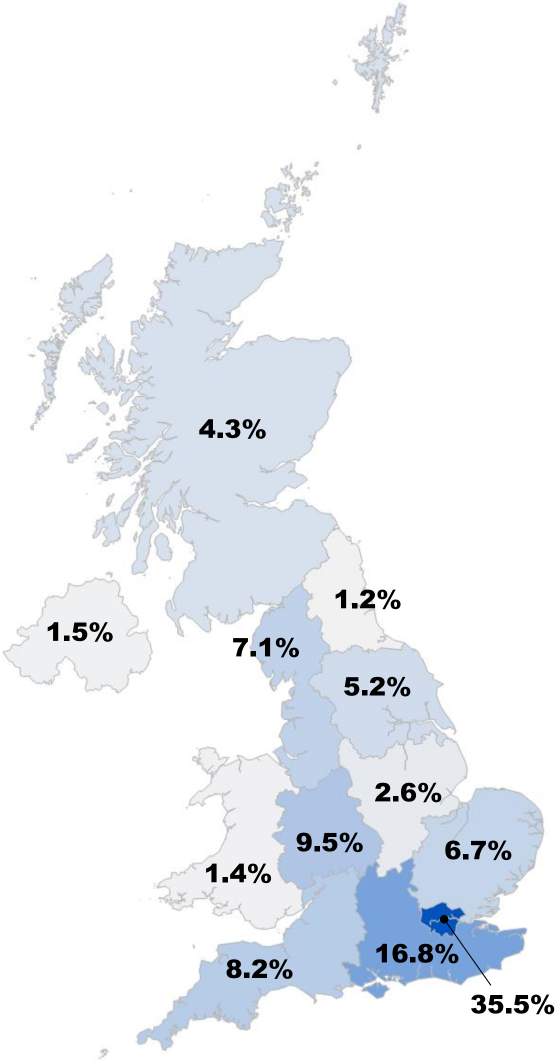
The darker the colour on the heatmap, the higher the density of cyber jobs in that region. This shows, as expected, a clustering of job posts in London and the South East.

[61] See https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020.
[62] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study.
[63] See https://www.tpdegrees.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf.

Figure 7.2: Percentage of core cyber job postings from each UK region

Ranking

1. Greater London (35.5%)
2. South East (16.8%)
3. West Midlands (9.5%)
4. South West (8.2%)
5. North West (7.1%)
6. East of England (6.7%)
7. Yorkshire and the Humber (5.2%)
8. Scotland (4.3%)
9. East Midlands (2.6%)
10. Northern Ireland (1.5%)
11. Wales (1.4%)
12. North East (1.2%)



Source: Burning Glass Technologies
Base: 105,194 core cyber job postings from September 2016 to August 2019
Map created using OpenStreetMap data in Mapbox

The regional differences in Figure 7.2 are very broad. They mask the fact that there are strong clusters of cyber security activity within regions. This is evidenced in the DCMS Cyber Sectoral Analysis 2020, which showed particularly strong sector hotspots within London, in parts of the North West, parts of the West Midlands and along the M4 corridor.[61]

We have, therefore, carried out more granular geographic analysis using the Travel to Work Areas (TTWAs) in the UK.[64] Figure 7.3 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.

[64] For an explanation of TTWAs, see the ONS website: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/traveltoworkareaanalysisingreatbritain/2016. There are a total of 228 TTWAs. The Isle of Man and the Channel Islands are not TTWAs so are not included. Our Location Quotient calculations are based on 2016 Annual Population Survey (APS) data, and the TTWA calculations are based on the April 2011 TTWAs.

Figure 7.3 again shows 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.

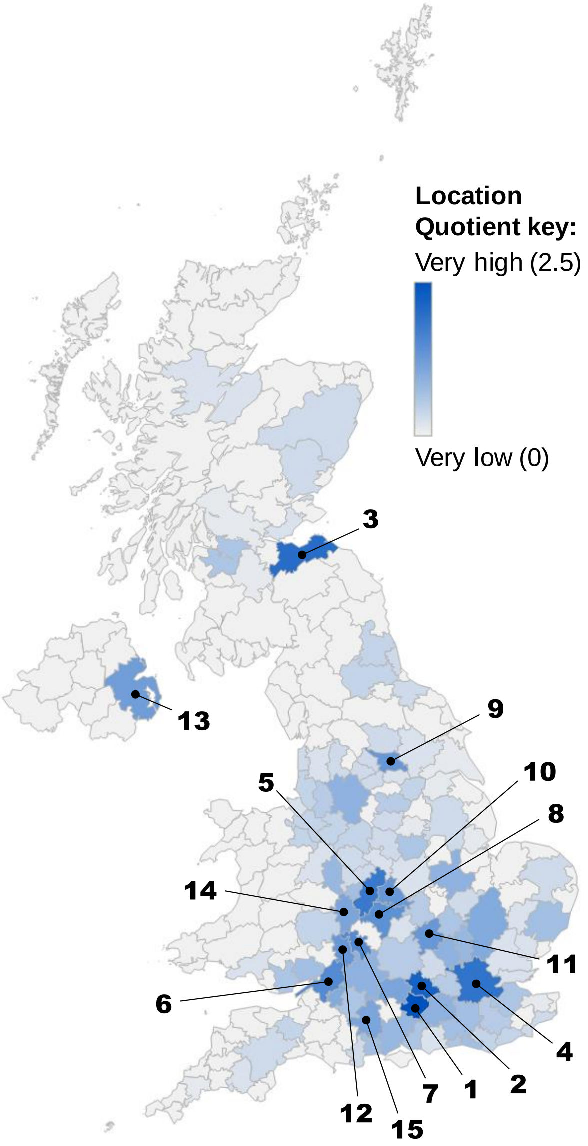
Figure 7.3: Number of core cyber job postings and Location Quotients in the top 15 UK Travel to Work Areas

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

i. London (8,474)
ii. Birmingham (1,360)
iii. Manchester (1,164)
iv. Edinburgh (684)
v. Bristol (682)
vi. Reading (624)
vii. Leeds (534)
viii. Belfast (529)
ix. Slough and Heathrow (398)
x. Glasgow (394)
xi. Cambridge (381)
xii. Coventry (371)
xiii. Luton (349)
xiv. Basingstoke (332)
xv. Southampton (302)

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

1. Basingstoke (2.5)
2. Reading (2.2)
3. Edinburgh (2.0)
4. London (1.9)
5. Birmingham (1.8)
6. Bristol (1.5)
7. Cheltenham (1.5)
8. Leamington Spa (1.4)
9. Leeds (1.3)
10. Coventry (1.3)
11. Milton Keynes (1.3)
12. Gloucester (1.3)
13. Belfast (1.2)
14. Worcester and Kidderminster (1.1)
15. Salisbury (1.1)



Source: Burning Glass Technologies
Base: 24,167 core cyber job postings from September 2018 to August 2019
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 also other cities like Edinburgh and Belfast. The analysis also highlights the strong demand for core cyber jobs across the West Midlands and the South West (in Bristol, Cheltenham and wider Gloucestershire).

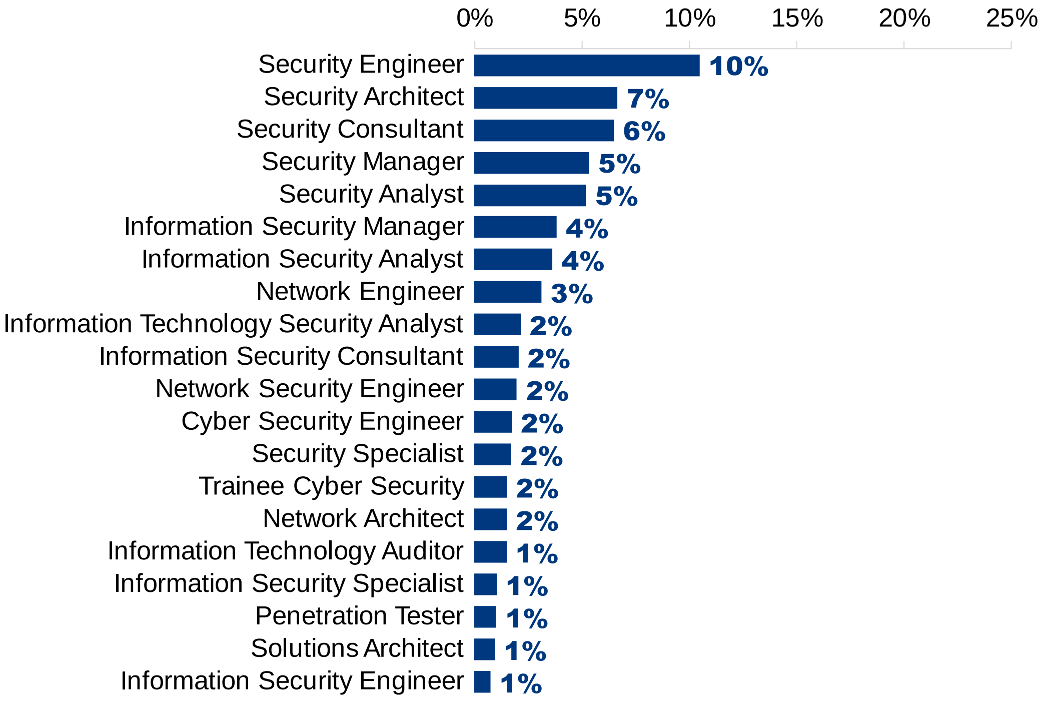
As a caveat to this geographic analysis, both Figures 7.2 and 7.3 may slightly underestimate the extent of cyber security labour market activity in certain regions. For example, DCMS's Cyber Sectoral Analysis 2020 found that 4 per cent of office locations in the cyber sector are in the East Midlands and a further 4 per cent are in Wales – neither of which register a high number of cyber security job postings in our analysis.[61] In locations like Wales, there are a small number of very large firms that dominate the local cyber security labour market. As we discuss in Chapter 6, the largest employers 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.

7.4 The job roles being advertised

Figure 7.4 lists the identified core cyber roles by job title. Many of these are minor variants of each other (e.g. Security Engineer and Network Engineer). It is possible to combine these categories to give a broader insight into the kinds of roles being recruited. We find that the most common roles requested are as follows (i.e. where the job title contains these specific terms):

- Security engineers (18%)
- Security analysts (13%)
- Security architects (10%)
- Security managers (9%)
- Security consultants (8%)

Figure 7.4: Top 20 recurring job titles among the 105,194 core cyber job roles identified

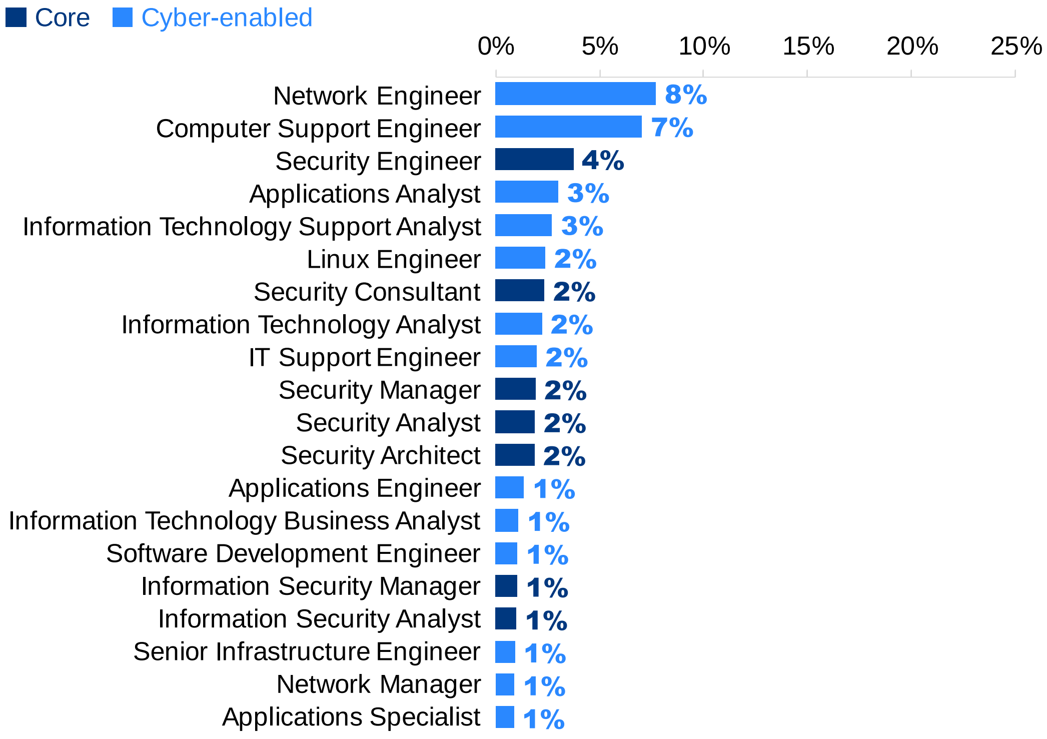


Source: Burning Glass Technologies
Base: 105,194 core cyber job postings from September 2016 to August 2019

Expanding this analysis out to cover all 393,257 identified job postings (covering the cyber-enabled job roles as well as the core roles), we can highlight some of the important enabling and complementary jobs that are well aligned to cyber security (Figure 7.5). These are often roles where the job descriptions state that knowledge of cyber or network security is desirable but not necessarily essential.

This highlights that employers are looking to build teams with not only dedicated cyber professionals, but also people working in complementary roles, such as support engineers and application analysts – people who will also require cyber security skills.

Figure 7.5: Top 20 recurring job titles among the 393,257 core and cyber-enabled job roles identified



Source: Burning Glass Technologies
Base: 393,257 core and cyber-enabled cyber job postings from September 2016 to August 2019

7.5 The sectors demanding cyber security staff

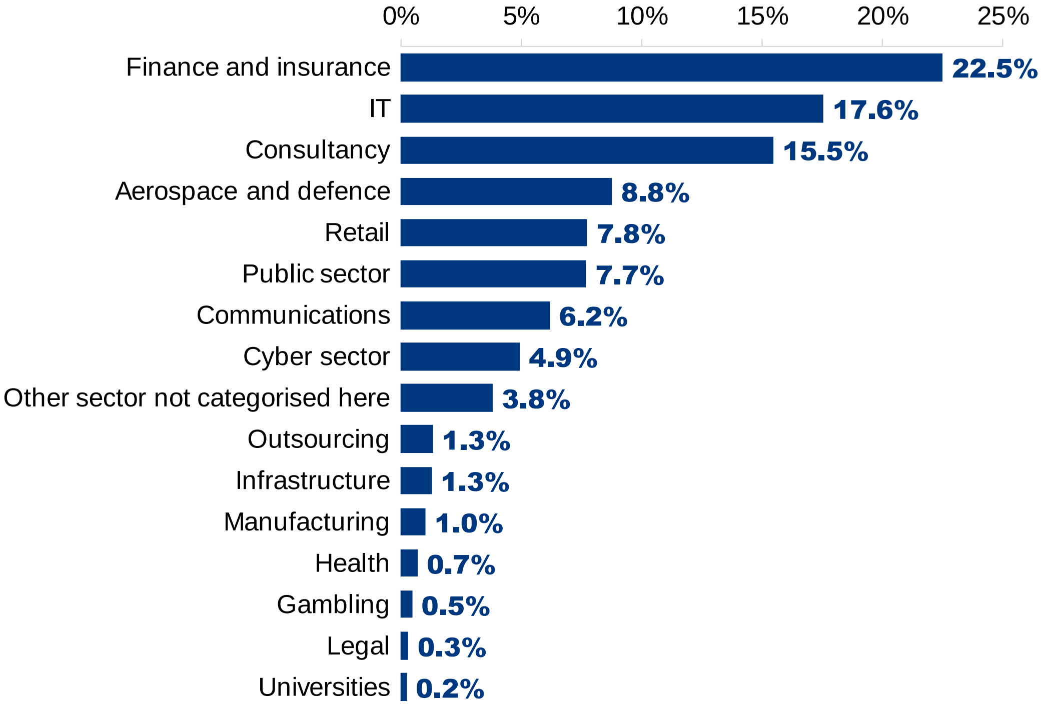
Job postings within the Burning Glass Technologies dataset are typically advertised through a recruitment agency. This means that the employer name – the end client of the recruitment agency – may not be contained within the job posting. However, for the core cyber roles, a total of 11,527 job postings (11% of all the core cyber job posts identified) have a known employer name[65] and have categorised these by their sector (Figure 7.6).[66]

As the smallest sectors that still enter the top 20 threshold account for under 1 per cent each, we show percentages to 1 decimal place for this chart.

[65] 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.

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

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



Source: Burning Glass Technologies
Base: 11,527 core cyber job postings from September 2016 to August 2019 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.

The retail sector appears relatively high on this list, which contrasts with the wider sector's low rankings in various questions in the survey. For example, cyber leads in this sector are less confident than average at carrying out various basic cyber security tasks in-house (see Chapter 4). However, our analysis shows that this recruitment is largely concentrated among 3 household name UK retailers.

Finally, matching the employers against the DCMS list of UK providers of cyber security products and services shows that 4.9 per cent of these 11,527 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 – strongly matching the narrative from the survey data in Chapter 6.

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 the core cyber roles, it is unsurprising that the key skill demanded from employers is knowledge of "information security" (61%) and "network security" (22%). This is very broad, possibly reflecting there is not yet a single, widely adopted cyber security skills framework to better break down the various skills areas. The full list is in Table 6.1.

Several of the skills requested are soft in nature, such as teamwork and collaboration (12%). The most commonly demanded technical skills areas include:

- Network engineering (e.g. Cisco and Juniper)
- Risk management and technical controls (e.g. ISO27001 and ITIL)
- Operating systems and virtualisation (e.g. Linux and VMWare)
- Cryptography
- Programming (e.g. Python, Java and SQL)

Table 7.1: Top skills requested for core cyber job roles

Skills	%	Skills	%	Skills	%
Information security	61%	IT industry knowledge	7%	VMware	5%
Network security	22%	UNIX	6%	Splunk	4%
ISO 27001	20%	Telecommunications	6%	Information assurance	4%
Cisco	17%	Microsoft Active Directory	6%	Network infrastructure (edge devices)	4%
LINUX	13%	Risk management	6%	Cisco switching	4%
Teamwork / collaboration	12%	Java	6%	Threat intelligence and analysis	4%
Security operations	11%	ISO standards	5%	Open web application security project	4%
ITIL	10%	Juniper networks	5%	DevOps	4%
Network engineering	10%	Software development	5%	The Open Group Architecture Framework (TOGAF)	4%
Project management	10%	Payment Card Industry (PCI)	5%	System or network configuration	4%
Customer service	10%	Budgeting	5%	Data security	4%
Stakeholder management	9%	Virtual Private Networking (VPN)	5%	Change management	3%
Cryptography	8%	Risk assessment	5%	Windows server	3%
Wide Area Network (WAN)	8%	Routers	5%	Cyber security knowledge	3%
Python	8%	Technical support	5%	Virtualisation	3%
Transmission Control Protocol (TCP) or Internet Protocol (IP)	7%	SQL	5%	Disaster recovery planning	3%
Information systems	7%	Domain Name System (DNS)	5%	Data privacy	3%

Source: Burning Glass Technologies
Base: 79,750 core cyber job postings from September 2016 to August 2019 that request specific skills

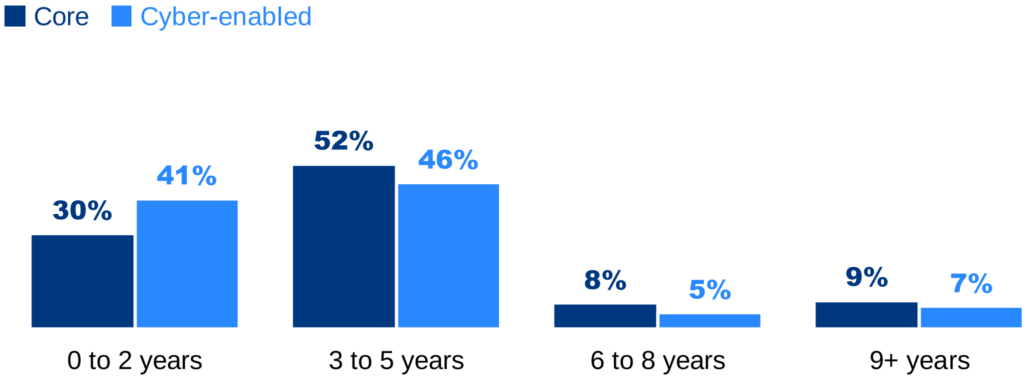
Experience requirements

Figure 7.7 demonstrates that, over the last 3 years, the most common request from employers looking to fill core cyber security roles has been for applicants with 3 to 5 years of experience (52%), followed by entry level applicants (30%). The greatest demand being for 3 to 5 years again strongly reflects the current snapshot of the cyber sector covered in Chapter 6.

In cyber-enabled roles, there is greater demand for those in entry level positions (41%, vs. 30% of core cyber job postings). This highlights the reluctance of employers to take on dedicated cyber staff at the entry level.

At the same time, it also highlights an opportunity – there may be further scope to explore how those entering cyber-enabled roles, like network technician or IT support roles, might be upskilled. For example, there could be a mapping of career pathways for those who join as a support technician after completing an IT degree or HND, build up industry experience, and learn the cyber security skills needed for a core cyber role via accredited training (e.g. CompTIA Network+ followed by CompTIA Security+).

Figure 7.7: 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): 16,044 core cyber job postings from September 2016 to August 2019; 55,915 cyber-enabled job postings

Education requirements

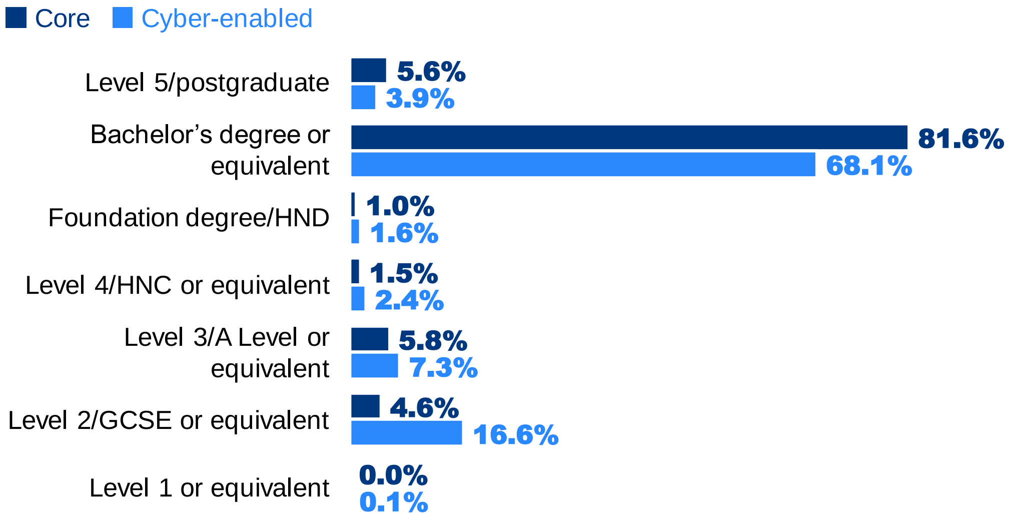
As Figure 7.8 shows, employers place a strong emphasis on applicants having bachelor's degrees or higher qualifications.

There is much less demand for foundation degrees and Higher National Certificates (HNCs) or other Level 4 certificates. The job postings that mention these are likely to be entry level roles that reflect where the employer is actually aware of these wider higher level qualifications.

There are differences between core and cyber-enabled job roles here as well. Employers looking to fill cyber-enabled job roles are twice as likely to accept A Levels or GCSEs as a minimum (24% vs. 11%). 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.

For core cyber roles, the 11 per cent of postings allowing applications from those with A Levels or GCSEs possibly reflects work and training schemes where applicants can earn and learn, such as the GCHQ and CNI degree apprenticeships. The proportion of core cyber job postings allowing for these as minimum qualifications rose from 9 per cent in 2017/18 to 12 per cent in 2018/19. Encouraging a wider range of employers to engage with these schemes could help to meet some of the labour demand.

Figure 7.8: 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): 19,085 core cyber job postings from September 2016 to August 2019; 60,373 cyber-enabled job postings

Demand for certifications

The most commonly requested certification is Certified Information Systems Security Professional (CISSP), which is included within 37 per cent of the job postings that ask for a specific certification. This reflects our qualitative findings in Chapter 2, which highlight 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 was 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

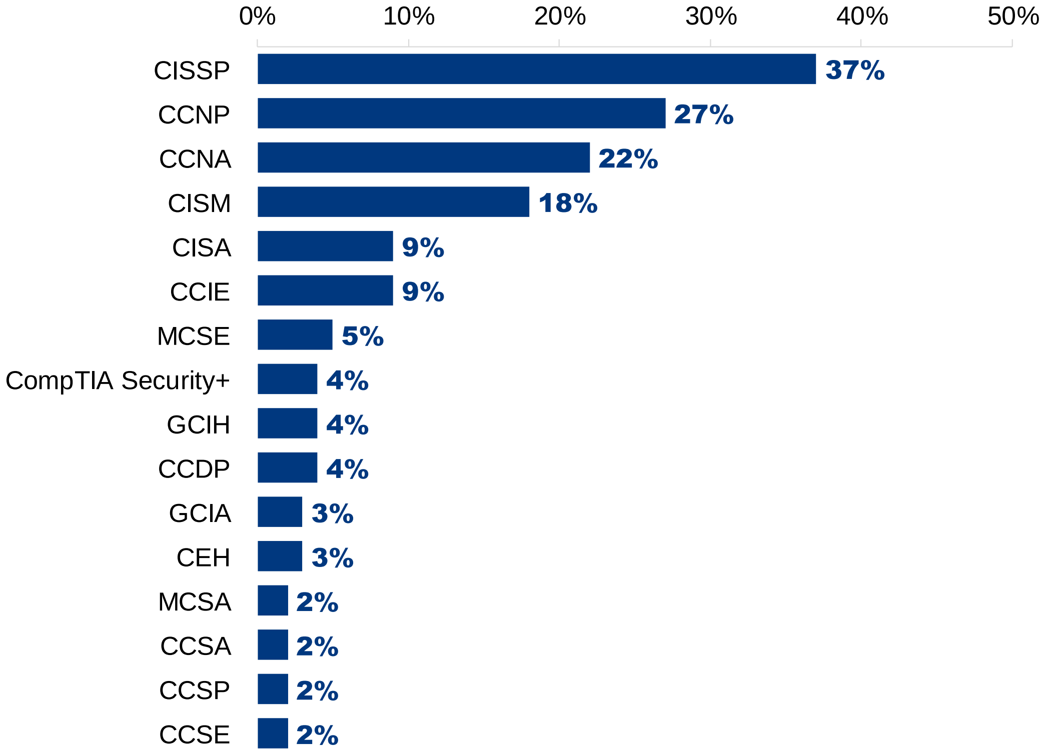
Cisco Certified Network certifications are also in high demand, with 27 per cent requesting Cisco Certified Network Professionals (CCNP), 22 per cent requesting Cisco Certified Network Associates (CCNA), and 9 per cent requesting Cisco Certified Internetwork Experts (CCIE). The top ranking certifications are shown in Figure 6.9.

The following certifications are not shown on the chart and were each mentioned in 1 per cent of job postings: GIAC Security Essentials (GSEC), PRINCE2, GIAC Certified Forensic Analyst (GCFA), Advanced Certificate in Programme and Project Support (ISEB), GIAC Reverse Engineering Malware (GREM), CompTIA A+ Certification, Cisco Certified Design Associate (CCDA), GIAC Penetration Tester (GPEN) and Microsoft Certified IT Professional (MCITP).

This analysis does not specify whether employers are requesting specific versions of the certifications shown in Figure 6.9. The version was often not specified in the job description – a further challenge for individuals navigating the training market.

All this demonstrates that the certifications requested can become rather specific and niche within cyber security job postings. Whilst job postings may include broad minimum educational requirements, the landscape can still be challenging for both employers and potential employees, needing to request and supply specific certifications to meet role expectations.

Figure 7.9: Percentage of core cyber job postings asking for the following certifications (where any certification is identified)



Source: Burning Glass Technologies
Base: 20,774 core cyber job postings from September 2016 to August 2019 that request specific certifications

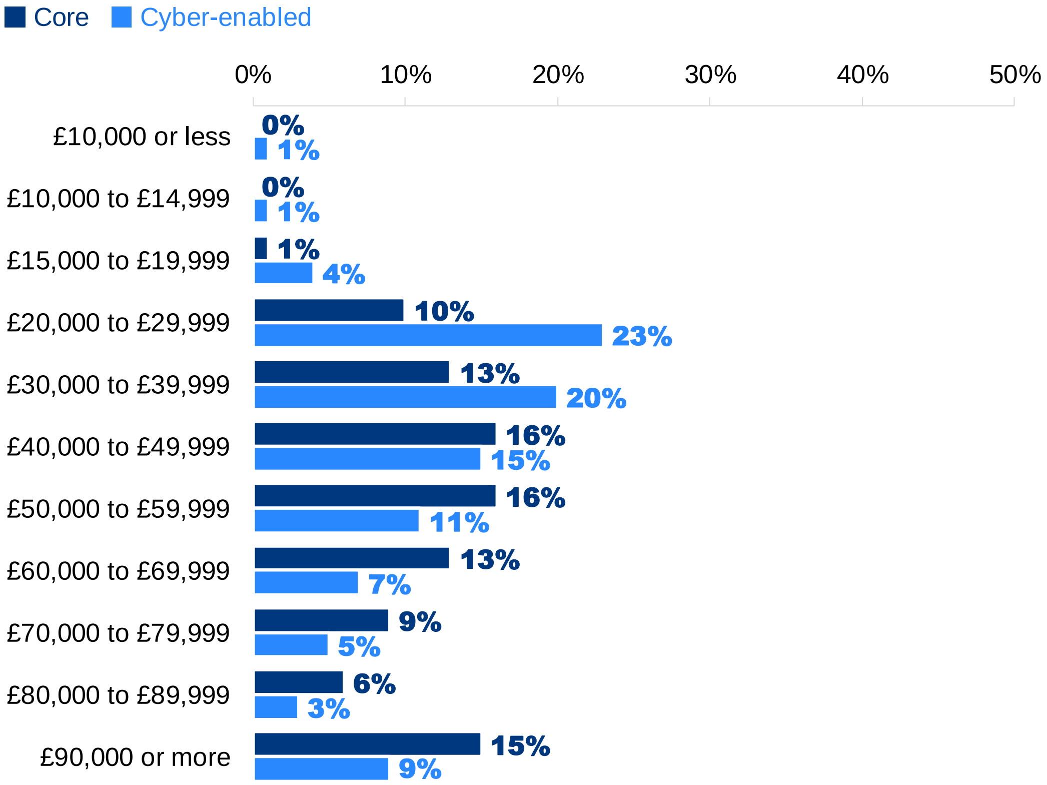
7.7 Salaries

Over the last 3 years, our analysis shows that 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 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 2019 was £47,934 (with a median of £40,063).[67] Using this value as a proxy for IT jobs in the UK suggests there is a wage premium of approximately 25-30 per cent for core cyber security jobs compared both to IT jobs as a whole, and jobs with a partial cyber security requirement.

Analysis of job postings with known salary data (Figure 7.10) demonstrates that the cyber-enabled jobs are typically lower paying, with almost 3 in 10 job posts advertised at less than £30,000 annually. By comparison, 9 in 10 core cyber jobs are advertised at *over* £30,000 annually.

Figure 7.10: Percentage of core and cyber-enabled job postings offering the following salaries (where the salary or salary range is advertised)



Source: Burning Glass Technologies
Bases (job postings that mention salaries or salary bands): 55,032 core cyber job postings from September 2016 to August 2019; 238,887 cyber-enabled job postings

[67] This is sourced from the Office for National Statistics (ONS, 2019) Annual Survey of Hours and Earnings, available at; https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/regionbyindustry2digitsicashetable5

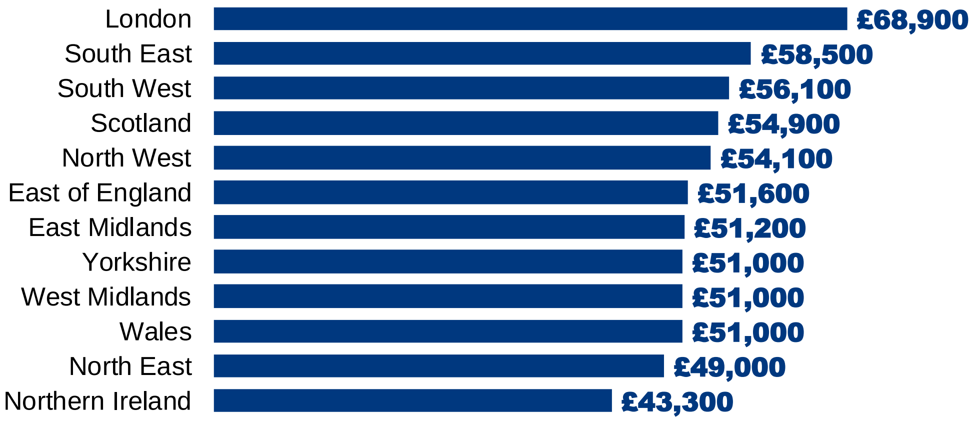
Geographic variation in salaries

London has 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, Northern Ireland has considerably lower average advertised salaries for core cyber security roles (a mean of £43,300).

Overall, typically core cyber job salaries are almost twice the level of average regional salaries[67], indicating that cyber security is a well paid career option within each region.

Figure 7.11: Mean salary offers for core cyber job postings, by region (where the salary or salary range is advertised)



Source: Burning Glass Technologies
Base: 55,032 core cyber job postings from September 2016 to August 2019 that mention salaries or salary bands

8 Outsourcing cyber security

This chapter looks at the organisations outside the cyber sector that outsource any aspects of their cyber security – what they outsource, their reasons for doing so and the challenges of managing external cyber security providers.

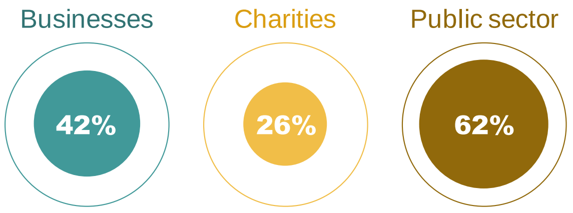
The wider context from external literature

- In general, the recent wider literature on cyber security skills does not cover outsourcing in detail. However, a 2019 Symantec survey of lead cyber professionals in the UK, France and Germany highlights the "externalisation" of cyber security – using managed service providers to handle key aspects – as a way for organisations to free up time for internal skills development and ease the recruitment burden[68]

8.1 The prevalence of outsourcing

As Figure 8.1 shows, around 4 in 10 businesses (42%) outsource any aspects of cyber security. This proportion is lower among charities and higher among public sector organisations.

Figure 8.1: Percentage of organisations that outsource any aspects of their cyber security to external providers



Bases: 1,046 businesses; 201 charities; 106 public sector organisations

It is worth noting that the Cyber Security Breaches Survey series has also consistently found that outsourcing is more common among businesses than charities, due to charities being less likely to feel they can afford to outsource.

Outsourcing is more common among non-micro businesses. In fact, more than half of all small (54%), medium (64%) and large businesses (64%) outsource part or all of their cyber security.

Outsourcing is more prevalent among sectors like finance and insurance (69%, vs. 44% on average) and education (46%). In contrast, information and communications businesses (27%) are less likely than others to outsource any aspects. These sector differences are consistent with those found in the 2018 survey. As per that earlier survey, 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 cyber security roles in-house.

[68] See https://resource.elq.symantec.com/LP=7421.

Change over time

Our survey finds that the percentage of businesses outsourcing has increased since 2018 (up by 12 percentage points from 30%). The Cyber Security Breaches Survey series, which tracks the prevalence of outsourcing through a different question, has not found any changes since 2016.[69] This suggests that the increase we see in this skills survey either represents a much more recent change in business behaviour, or that it is a one-off result that may not be replicated in future surveys.

8.2 What aspects of cyber security do organisations outsource?

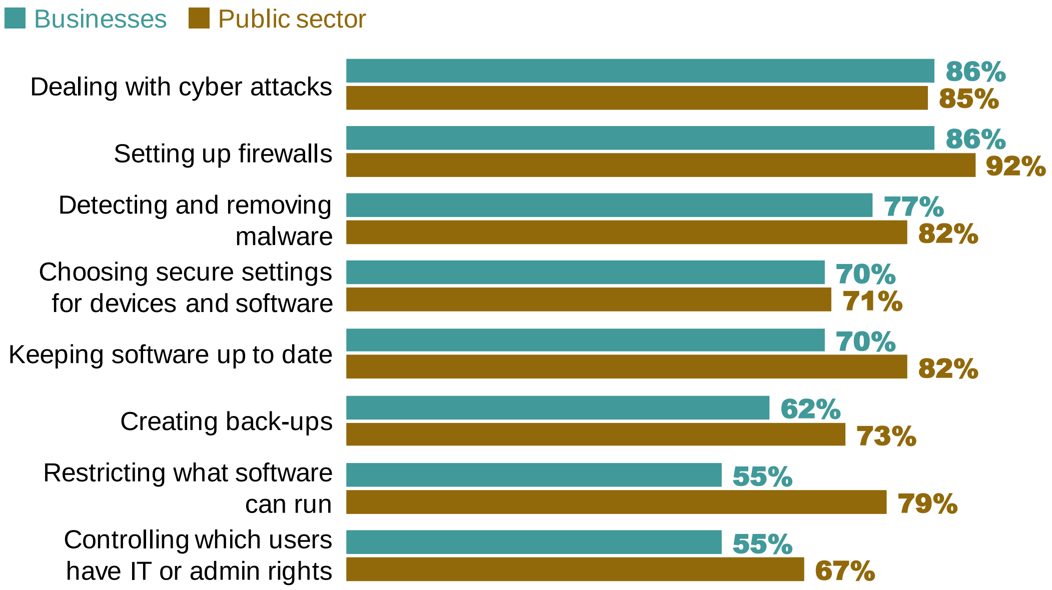
Outsourcing basic functions

Figure 8.1 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. Here, we have focused on businesses and public sector organisations, given the very small sample of charities that outsource any aspects.

Two very commonly outsourced functions, each in over three-quarters of the cases where anything is outsourced, are firewalls and malware detection and removal. The basic functions that tend to be less commonly outsourced are around restricting software access and control of IT admin rights.

Among those that outsource, just a third (33%) of businesses outsource all the basic aspects of their cyber security (including incident response). This is more common for public sector organisations – half (48%) of the ones that outsource say they outsource all the basic aspects.

Figure 8.2: Percentage of organisations outsourcing various basic cyber security functions, among those that outsource any aspects



Bases: 496 businesses that outsource cyber security; 62 public sector organisations that outsource cyber security

Outsourcing more advanced functions

Figure 8.3 shows the kinds of advanced functions that get outsourced, among the organisations that outsource any aspects of cyber security. This reflects the split used across this study in terms of basic

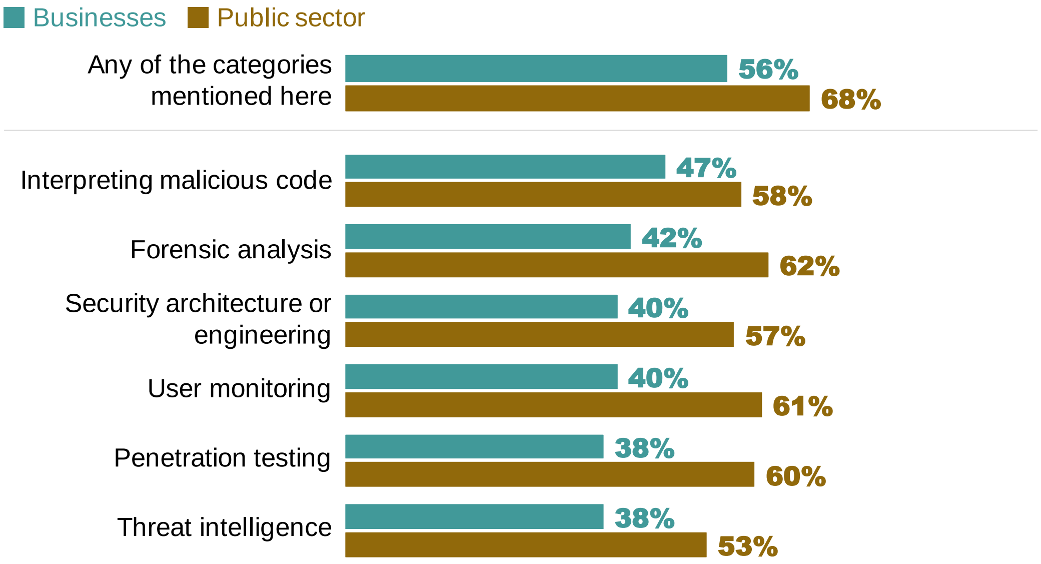
[69] See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.

versus advanced technical cyber security skills (which links back to the definition and categorisation of cyber security skills established in the 2018 study).

As with the previous section, we focus on businesses and public sector organisations. The charity sample is too small to report at this question.

In general, public sector organisations tend to outsource more of these advanced kinds of tasks than businesses. For both groups, there are no specific tasks among this list that are considerably more or less likely to be kept in-house.

Figure 8.3: Percentage of organisations outsourcing various advanced cyber security functions, among those that outsource any aspects



Bases: 496 businesses that outsource cyber security; 62 public sector organisations that outsource cyber security

8.3 Reasons for outsourcing aspects of cyber security

In the qualitative research, there were various reasons behind outsourcing decisions:

- Outsourcing let organisations access specialist technical skills and accreditations. Penetration testing was commonly mentioned, as this required specific certifications that in-house staff lacked
- It was sometimes a way of offloading resource intensive, high volume work, so that in-house staff could focus on more strategic activities. One example given was creating and deleting user IDs, where the cyber lead felt it was a better use of their in-house resource to provide the governance framework for this and then let a third party manage the work
- For some, outsourcing offered independent cyber security assurance. This was mentioned, for example, with regards to cyber audits, where one cyber lead felt it was important to have an outside voice highlighting the areas where the organisation could improve
- Getting in short term contractors was often considered a more cost effective and instantaneous solution relative to the investment cost and time delay of recruiting and training in-house teams

8.4 Challenges faced around outsourcing

In the qualitative research, where aspects of cyber security had been outsourced, the challenges that organisations faced differed greatly across interviews, based on the nature of the work outsourced, the business context and the terms governing the outsourcing relationship. There were, therefore, few common themes. However, these are some examples of the unique challenges some teams faced:

- In one case, an interviewee discussed their external cyber security provider that had a wide-ranging monitoring role. The provider was moving towards a more automated approach potentially looking to employ fewer skilled staff in the future. The interviewee was concerned about the lack of understanding of their strategic business priorities shown by the external provider. They also felt that the provider did not fully appreciate the reputational and financial implications if key customer facing aspects of the business were to ever be taken down. They intended to bring monitoring functions partly in-house, so that third party monitoring would only be used for assurance rather than as a first line of defence

- One interviewee said that it was difficult for them to measure success with their external provider, which oversaw all the operational aspects of their cyber security. They had standard service level agreements based on how fast the provider could implement changes. They also considered success in terms of the number of viruses in the business or number of breaches that had been shut down. However, in their view, these did not measure the more fundamental objective, which was to do with improving the organisation’s “security posture” and the staff culture

- Finally, one cyber lead in a large business discussed a situation where the decision to outsource aspects of cyber security was unavoidable, even though they would have preferred to keep these functions in-house to better control the risks. The situation was brought about through mergers and the legacy of ownership of the business. Another firm owned the infrastructure and equipment used by this business, and this other firm was responsible for the cyber security of these things. To take these functions in-house, the business would have to buy out the current provider

9 Conclusions and recommendations

This latest study into the UK cyber security labour market builds considerably on the initial work carried out in 2018. Many of the key insights from 2018 – for example, around the large number of people working informally in cyber roles – are reinforced here. We also cover several areas in far greater depth this time, such as hard-to-fill vacancies, workforce diversity and regional demand for skills.

With roughly a year's gap between the two studies, we would not expect to see any major changes over this time. In general, the findings are very consistent. Nevertheless, it is encouraging to see small improvements across the business population. This includes:

- Fewer businesses reporting basic technical skills gaps (down from 54% to 48%)
- An increase in the proportion of businesses that have carried out a formal analysis of their cyber security training needs (from 14% to 22%)
- An increase in the proportion of businesses that consider it essential to have incident response skills (17% to 23%)

The rest of this chapter lays out the most important broad themes emerging from the 2020 study and our recommendations off the back of these findings:

- **Cyber security skills gaps and skills shortages continue to affect a large number of organisations, both within and outside the cyber sector.** Approximately 653,000 businesses have a basic skills gap, lacking the confidence to carry out basic cyber security tasks. Roughly 408,000 businesses have more advanced skills gaps, in areas such as penetration testing, forensic analysis and security architecture. Skills gaps affect cyber sector organisations as well, preventing most of them from fully achieving their business goals

- **Cyber teams are looking for people with a holistic skillset.** This includes not only technical skills but also soft skills, such as communication skills, consultancy skills, people management and the ability to train others. It is this combination that organisations find especially challenging to recruit. There is also a difference between having technical knowledge, and the ability to implement that technical knowledge in a business context. Organisations want people who can not only describe a cyber security audit, for example, but understand the practical challenges they will face when carrying out an audit in a business environment

- **There continues to be a lack of investment in technical skills and training.** This is not simply among micro businesses that cannot afford big training budgets. The overwhelming majority of large businesses have not sent their cyber staff on training in the past year. Two-fifths of cyber sector businesses do not employ staff with relevant qualifications or certifications, or are unsure if their staff are qualified. Cyber security training for wider (non-cyber) staff in the private sector is also very rare, especially among smaller businesses

- **The cyber security labour market is challenging to navigate.** Cyber security is a constantly evolving discipline, meaning that university degree and postgraduate courses risk becoming out of date. There are also a plethora of qualifications and certifications, driven by the increasingly large number of product vendors. It is difficult for employers and job applicants to assess the quality of courses and other training products, and quality tends to vary greatly. The National Cyber Security Centre (NCSC) is seen as a reputable voice to help guide people through this landscape

- **Employers lack awareness of the government's existing cyber security skills initiatives.** This includes schemes such as CyberFirst and the Cyber Skills Immediate Impact Fund. Where there was awareness, there was often a desire to see such schemes expanded and to make them more joined up. This includes showing how different initiatives relate to one another, and how they fit into a broader career pathway from school to employment

- **Recruitment agencies and education institutions lack awareness of employers' needs.** Schools, colleges and universities are often perceived to have a narrow understanding of cyber security careers, and could improve the careers guidance they offer in this area. Similarly, recruitment agencies need to improve their understanding of the labour market and the kinds of skills and qualifications that employers need

- **Many employers could benefit from broadening their recruitment practices.** Organisations have had success when they have shifted their focus towards career starters, apprentices and graduates, those transitioning from other sectors or roles outside cyber security, and other diverse groups. Currently, many are limiting themselves to a small recruitment pool of job applicants who are already in cyber roles, typically with 3 to 5 years of experience. Employers need support to find apprentices and train them up. Individuals transitioning into cyber security also need support when figuring out which career pathways and job roles best suit their existing skills, and which qualifications or accreditations they need to enter these roles

- **Discussions around workforce diversity need reframing.** Relatively few cyber sector businesses say they have adapted their recruitment processes or carried out any specific activities to encourage applications from diverse groups. This is partly because they lack awareness of what they could do. They also lack awareness of specific groups, such as the neurodivergent. Moreover, employers often underplay one of the most fundamental benefits of a diverse workforce – it is a way for organisations to widen their recruitment pool and tackle skills gaps

- **There are geographic hotspots of activity in the cyber security labour market.** These hotspots include London, Edinburgh and Belfast, as well as parts of the West Midlands and the South West, such as Bristol, Cheltenham and wider Gloucestershire. These hotspots have large variations that may also be worth exploring in more detail in future studies. Their existence also suggests that addressing skills shortages will require a regional approach

Recommendations

The following recommendations are all based on the evidence generated from this study. It will require engagement from government, the cyber sector and other cyber employers outside the sector, education institutions and recruitment agencies to take them forward. As the UK Cyber Security Council grows and develops, it is likely to be a major contributor in this space. Therefore, we have opted in most cases to not assign responsibility for each recommendation to a specific group, as it is up to government and industry to decide and agree their respective roles.

Improving awareness and participation in government initiatives

Recommendation 1: The entire programme of government activity on cyber security skills should be joined up under a cohesive brand. Employers and individuals in the cyber security labour market should have clarity over how different initiatives relate to one another and how they fit into a broader career pathway from school to employment.

Recommendation 2: There should be further work to explore how schemes such as CyberFirst can be made more widely available to young people and attract as broad a pool as possible.

Improving the pipeline through education

Recommendation 3: There should be further work with schools and universities to improve their understanding of the breadth of career opportunities in cyber security, so they can promote these careers more effectively to a wider range of young people.

Recommendation 4: Universities that offer courses in cyber security should work with the cyber sector to ensure that these courses adapt to the evolving needs of the sector, provide students with a more practical understanding of cyber security in a business context and build the soft skills that employers require. In addition, more of these universities and cyber sector employers should, where relevant, offer longer work placements (measured in months rather than weeks).

Training and apprenticeships

Recommendation 5: There should be case studies of cyber employers that have used on-the-job training and work shadowing effectively, to get new joiners, apprentices and those transitioning from non-cyber roles to be job ready. The UK Cyber Security Council may have a role in producing and sharing these case studies.

Recommendation 6: There should be a consistent approach – one that can feasibly be scaled up – for promoting and endorsing high-quality cyber security training providers and courses to cyber employers and individuals. This could, for example, involve expanding the existing GCHQ Certified Training scheme.

Recommendation 7: There should be further guidance for recruitment agents, or partnerships between agents and cyber employers, to improve their understanding of the requirements for different cyber roles. This could include, for example, guidance around how to use roles frameworks.

Recommendation 8: There should be more engagement with cyber employers to better understand the challenges they face when seeking apprentices in cyber roles, and to encourage greater uptake. This could build on ongoing work to develop new apprenticeship standards for cyber roles.

Recommendation 9: There should be a review of the existing range of cyber security training courses. This would assess the extent to which these courses provide employers and training recipients with the necessary technical, practical and soft skills to work in cyber roles. It would help to guide the employers and individuals seeking training. The UK Cyber Security Council may have a role in such a review.

Recommendation 10: There should be further promotion of the NCSC eLearning package[70], particularly to raise awareness among wider (non-cyber) staff in small and medium enterprises (SMEs).

Broadening recruitment practices

Recommendation 11: Cyber sector businesses should be encouraged to broaden their recruitment, to look beyond job applicants that have 3 to 5 years of experience. This includes apprenticeships and other work placements, starting graduate schemes or other opportunities for career starters, and recruiting

[70] See https://www.ncsc.gov.uk/information/certified-training.

from more diverse groups. This involves adapting recruitment processes and, where feasible, being flexible with job specifications and minimum requirements, to encourage a wider range of applicants.

Recommendation 12: As part of the ongoing work to map cyber security career pathways, there should be a focus on developing the pathways for those moving from non-cyber roles into cyber ones. The mapping should help these individuals – wider IT professionals, as well as people from more diverse career backgrounds, such as former members of the armed forces – to understand the kinds of roles that best fit their existing skillsets, and the qualifications that will support their transition to cyber security.

Recommendation 13: There should be further engagement with cyber employers based outside of geographic hotspots in the cyber security labour market (such as London and parts of the West Midlands), to better understand the recruitment barriers and challenges they might face as a result of their locations.

Improving workforce diversity

Recommendation 14: There should be guidance and best practice examples provided to the heads of cyber teams on how to improve diversity in recruitment, and how to make working environments more attractive for diverse groups.

Recommendation 15: Communications around diversity in cyber security should be reframed, to focus more on how a diverse workforce can address skills gaps. This could be through a communications campaign, sharing positive case studies.

References

Collier and Martin (2019) Beyond Awareness: The Breadth and Depth of the Cyber Skills Demand, Centre for Technology and Global Affairs, University of Oxford (https://www.ctga.ox.ac.uk/article/beyond-awareness-breadth-and-depth-cyber-skills-demand)

Donaldson, Hobson, Pedley, Shah, Crozier and Furnell (2020) UK Cyber Security Sectoral Analysis 2020, Department for Digital, Culture, Media & Sport (https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020)

EY (2018) Global Information Security Survey 2018-19 (https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf)

Ipsos MORI (2019) Cyber Security Breaches Survey 2019: Main report, Department for Digital, Culture, Media & Sport (https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019)

ISACA (2019) State of Cybersecurity 2019 (https://cybersecurity.isaca.org/state-of-cybersecurity)

ISC2 (2019) Cybersecurity Workforce Study 2019 (https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study)

ISC2 (2018) Cybersecurity Workforce Study 2018 (https://www.isc2.org/research)

Malan, Lale-Demoz, Rampton (2018) Identifying the Role of Further and Higher Education in Cyber Security Skills Development, Department for Digital, Culture, Media & Sport and Centre for Strategy & Evaluation Services (https://www.gov.uk/government/publications/the-role-of-further-and-higher-education-in-cyber-security-skills)

Oltsik (2019) The Life and Times of Cybersecurity Professionals 2018, Enterprise Security Group and Information Systems Security Association (https://www.esg-global.com/esg-issa-research-report-2018)

Raywood (2019) State of Cybersecurity Report 2019, InfoSecurity Magazine (https://www.infosecurity-magazine.com/white-papers/state-of-cybersecurity-report-2019-1/)

Symantec (2019) High Alert: Tackling Cyber Security Overload in 2019 (https://resource.elq.symantec.com/LP=7421)

Tech Partnership (2017) Factsheet: Cyber Security Specialists in the UK (https://www.tpdegrees.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf)

Wilson (2019) The Security Profession in 2018/19, Chartered Institute of Information Security (https://www.ciisec.org/CIISEC/Resources/White_Papers/CIISEC/Resources/White_Papers)

Winterbotham, Vivian, Kik, Huntley Hewitt, Tweddle, Downing, Thomson, Morrice and Stroud (2018) Employer Skills Survey 2017, Department for Education (https://www.gov.uk/government/publications/employer-skills-survey-2017-uk-report)

Ipsos MORI's 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.

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.

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.

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.

Data Protection Act 2018

Ipsos MORI is required to comply with the Data Protection Act 2018. It covers the processing of personal data and the protection of privacy.

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.